NWA-1100

802.11b/g Wireless Access Point

User's Guide

Default Login Details

IP Address	http://192.168.1.2
Password	1234

Firmware Version 3.6
Edition 2, 2/2009

ZyXEL

www.zyxel.com

Copyright © 2009
ZyXEL Communications Corporation

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the ZyXEL Device using the web configurator. You should have at least a basic knowledge of TCP/IP networking concepts and topology.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get up and running right away. It contains information on setting up your network and configuring for Internet access.

- Supporting Disk

  Refer to the included CD for support documents.

- ZyXEL Web Site

  Please refer to www.zyxel.com for additional support documentation and product certifications.

User Guide Feedback

Help us help you. Send all User Guide-related comments, questions or suggestions for improvement to the following address, or use e-mail instead. Thank you!

The Technical Writing Team,
ZyXEL Communications Corp.,
6 Innovation Road II,
Science-Based Industrial Park,
Hsinchu, 300, Taiwan.

E-mail: techwriters@zyxel.com.tw

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device. See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.

Brief description of the problem and the steps you took to sol

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

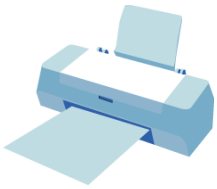
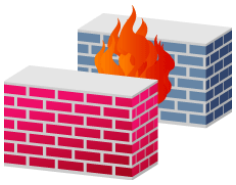
Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The NWA-1100 may be referred to as the "ZyXEL Device", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Configuration File > Backup** means you first click **Maintenance** in the navigation panel, then the **Configuration File** sub menu and finally the **Backup** button to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The ZyXEL Device icon is not an exact representation of your device.

ZyXEL Device	Computer	Notebook computer
Server	Printer 	Firewall 
Ethernet Switch	Switch	Router

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- ONLY qualified service personnel should service or disassemble this device.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.
- The PoE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

Introduction **17**

Introducing the ZyXEL Device 19
Introducing the Web Configurator 29
Status Screens 33
Tutorial 37

The Web Configurator **45**

System Screens 47
Wireless Settings Screen 55
Wireless Security Screen 73
RADIUS Screen 89
MAC Filter Screen 93
IP Screen 97
Remote Management 101
Certificate Screen 111
Log Screens 115
Maintenance 123
Troubleshooting 131

Appendices and Index **137**

Table of Contents

About This User's Guide **3**

Document Conventions **5**

Safety Warnings **7**

Contents Overview **9**

Table of Contents **11**

Part I: Introduction **17**

Chapter 1
Introducing the ZyXEL Device **19**

1.1 Introducing the ZyXEL Device 19
1.2 Applications for the ZyXEL Device 19
1.2.1 Access Point 20
1.2.2 Wireless Client 21
1.2.3 Bridge 21
1.2.4 AP + Bridge 24
1.3 Ways to Manage the ZyXEL Device 25
1.4 Configuring Your ZyXEL Device's Security Features 25
1.4.1 Control Access to Your Device 25
1.4.2 Wireless Security 26
1.5 Good Habits for Managing the ZyXEL Device 26
1.6 Hardware Connections 26
1.7 LEDs 27

Chapter 2
Introducing the Web Configurator **29**

2.1 Accessing the Web Configurator 29
2.2 Resetting the ZyXEL Device 30
2.2.1 Methods of Restoring Factory-Defaults 30
2.3 Navigating the Web Configurator 30

Chapter 3
Status Screens **33**

3.1 The Status Screen 33

3.1.1 System Statistics Screen 35

Chapter 4
Tutorial 37

4.1 How to Configure the Wireless LAN 37
4.1.1 Choosing the Wireless Mode 37
4.1.2 Wireless LAN Configuration Overview 37
4.1.3 Further Reading 38
4.2 ZyXEL Device Setup in Wireless Client Mode 39
4.2.1 Scenario 39
4.2.2 Configuring the ZyXEL Device in Access Point Mode 39
4.2.3 Configuring the ZyXEL Device in Wireless Client Mode 41
4.2.4 Testing the Connection and Troubleshooting 44

Part II: The Web Configurator 45

Chapter 5
System Screens 47

5.1 Overview 47
5.2 What You Can Do in the System Screens 47
5.3 What You Need To Know About the System Screens 48
5.4 General Screen 49
5.4.1 Password Screen 50
5.5 Time Screen 51
5.6 Technical Reference 53
5.6.1 Pre-defined NTP Time Servers List 53

Chapter 6
Wireless Settings Screen 55

6.1 Overview 55
6.2 What You Can Do in the Wireless Settings Screen 56
6.3 What You Need To Know About Wireless Settings Screen 56
6.4 Wireless Settings Screen 57
6.4.1 Access Point Mode 58
6.4.2 Wireless Client Mode 61
6.4.3 Bridge Mode 63
6.4.4 AP + Bridge Mode 67
6.5 Technical Reference 68
6.5.1 WMM QoS 68
6.5.2 Spanning Tree Protocol (STP) 68
6.5.2.1 Rapid STP 68

6.5.2.2 STP Terminology 69
6.5.2.3 How STP Works 69
6.5.2.4 STP Port States 70
6.5.3 Additional Wireless Terms 70

Chapter 7
Wireless Security Screen 73

7.1 Overview 73
7.2 What You Can Do in the Wireless Security Screen 73
7.3 What You Need To Know About Wireless Security 74
7.4 The Security Screen 76
7.4.1 Security: WEP 77
7.4.2 Security: 802.1x Only 78
7.4.2.1 Access Point 78
7.4.2.2 Wireless Client 80
7.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit 81
7.4.4 Security: WPA 82
7.4.4.1 Access Point 83
7.4.4.2 Wireless Client 84
7.4.5 Security: WPA2 or WPA2-MIX 84
7.4.5.1 Access Point 85
7.4.5.2 Wireless Client 86
7.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX 87
7.5 Technical Reference 87

Chapter 8
RADIUS Screen 89

8.1 Overview 89
8.2 What You Can Do in the RADIUS Screen 89
8.3 What You Need to Know About RADIUS 90
8.4 The RADIUS Screen 90

Chapter 9
MAC Filter Screen 93

9.1 Overview 93
9.2 What You Can Do in the MAC Filter 93
9.3 What You Need To Know About MAC Filter 94
9.4 MAC Filter Screen 94

Chapter 10
IP Screen 97

10.1 Overview 97
10.2 What You Can Do in the IP Screen 97

10.3 What You Need to Know About IP 98
10.4 IP Screen 98
10.5 Technical Reference 99
10.5.1 WAN IP Address Assignment 99

Chapter 11
Remote Management 101

11.1 Overview 101
11.2 What You Can Do in the Remote Management Screens 102
11.3 What You Need To Know About Remote Management 102
11.4 The Telnet Screen 104
11.5 The FTP Screen 105
11.6 The WWW Screen 106
11.7 The SNMP Screen 107
11.8 Technical Reference 108
11.8.1 MIB 109
11.8.2 Supported MIBs 109
11.8.3 SNMP Traps 109

Chapter 12
Certificate Screen 111

12.1 Overview 111
12.2 What You Can Do in the Certificate Screen 111
12.3 What You Need To Know About Certificates 111
12.4 Certificate Screen 112
12.5 Technical Reference 113
12.5.1 Private-Public Certificates 113
12.5.2 Certification Authorities 113
12.5.3 Checking the Fingerprint of a Certificate on Your Computer 114

Chapter 13
Log Screens 115

13.1 Overview 115
13.2 What You Can Do in the Log Screens 116
13.3 What You Need To Know About Logs 116
13.4 View Log Screen 116
13.5 Log Settings Screen 117
13.6 Technical Reference 120
13.6.1 Example Log Messages 120
13.7 Log Commands 121
13.7.1 Configuring What You Want the ZyXEL Device to Log 121
13.7.2 Displaying Logs 121
13.7.3 Command List 121

Chapter 14
Maintenance 123

14.1 Overview 123
14.2 What You Can Do in the Maintenance Screens 123
14.3 What You Need To Know About the Maintenance Screens 123
14.4 Association List Screen 124
14.5 Channel Usage Screen 124
14.6 F/W Upload Screen 126
14.7 Configuration Screen 127
14.7.1 Backup Configuration 128
14.7.2 Restore Configuration 128
14.7.3 Back to Factory Defaults 130
14.8 Restart Screen 130

Chapter 15
Troubleshooting 131

15.1 Power, Hardware Connections, and LEDs 131
15.2 ZyXEL Device Access and Login 132
15.3 Internet Access 134

Part III: Appendices and Index 137

Appendix A Product Specifications 139
Appendix B Power over Ethernet (PoE) Specifications 141
Appendix C Power Adaptor Specifications 143
Appendix D Setting up Your Computer's IP Address 145
Appendix E Wireless LANs 157
Appendix F Pop-up Windows, JavaScripts and Java Permissions 173
Appendix G IP Addresses and Subnetting 181
Appendix H Text File Based Auto Configuration 191
Appendix I How to Access and Use the CLI 199
Appendix J Open Software Announcements 203
Appendix K Legal Information 215

Index 219

PART I
Introduction

Introducing the ZyXEL Device (19)

Status Screens (33)

Introducing the Web Configurator (29)

Tutorial (37)

1

Introducing the ZyXEL Device

This chapter introduces the main applications and features of the ZyXEL Device. It also discusses the ways you can manage your ZyXEL Device.

1.1 Introducing the ZyXEL Device

Your ZyXEL Device extends the range of your existing wired network without additional wiring, providing easy network access to mobile users.

It controls network access with MAC address filtering and RADIUS server authentication.It also provides a high level of network traffic security, supporting IEEE 802.1x, Wi-Fi Protected Access (WPA), WPA2 and WEP data encryption. Its Quality of Service (QoS) features allow you to prioritize time-sensitive or highly important applications such as VoIP.

Your ZyXEL Device is easy to install, configure and use. The embedded Web-based configurator enables simple, straightforward management and maintenance.

See the Quick Start Guide for instructions on how to make hardware connections.

1.2 Applications for the ZyXEL Device

The ZyXEL Device can be configured to use the following WLAN operating modes

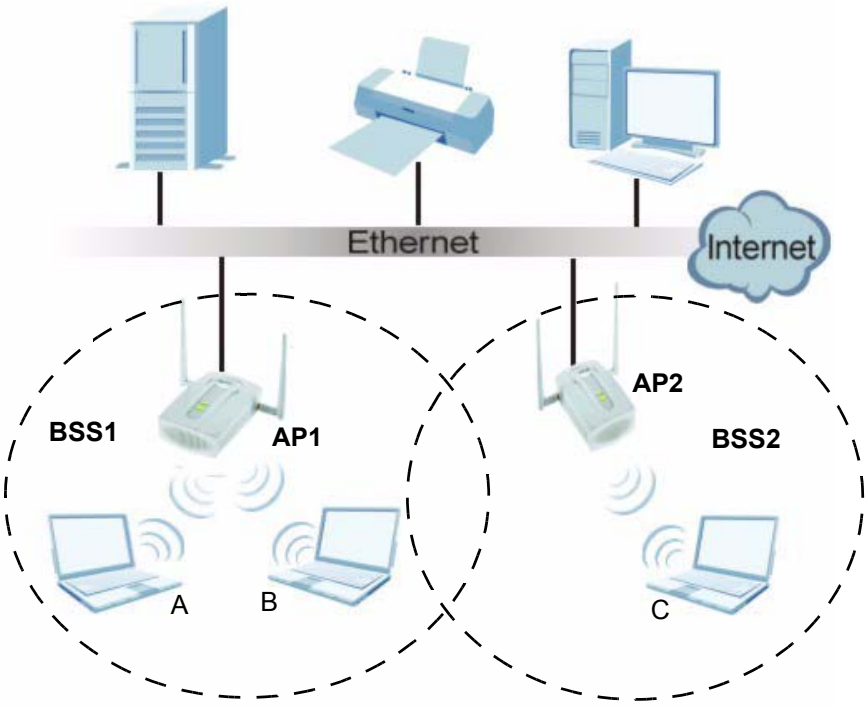
1. AP (Access Point)
2. Wireless Client
3. Bridge
4. AP + Bridge

Applications for each operating mode are shown below.

1.2.1 Access Point

The ZyXEL Device is an ideal access solution for wireless Internet connection. A typical Internet access application for your ZyXEL Device is shown as follows. Stations A, B and C can access the wired network through the ZyXEL Devices.

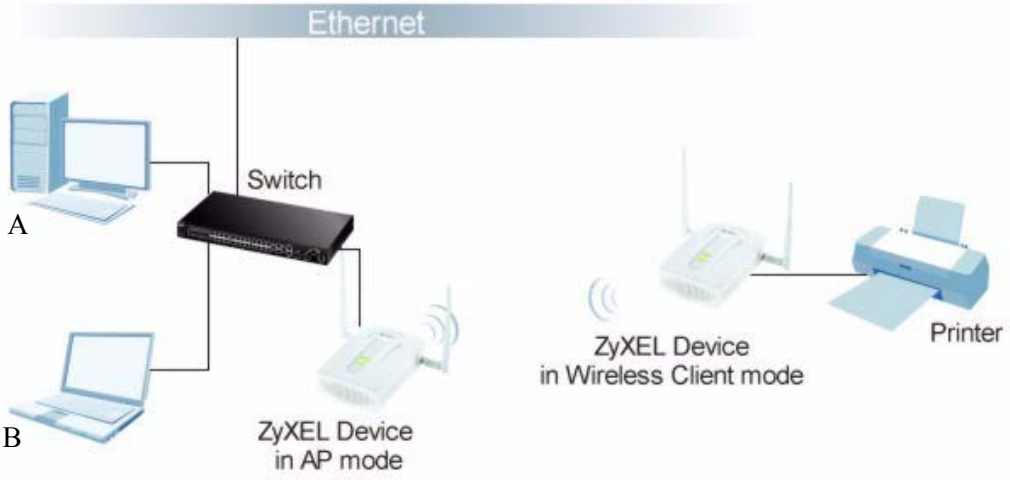
Figure 1 Access Point Application



1.2.2 Wireless Client

The ZyXEL Device can be used as a wireless client to communicate with an existing network. In the figure below, the printer can receive requests from the wired computer clients A and B via the ZyXEL Device in Wireless Client mode.

Figure 2 Wireless Client Application



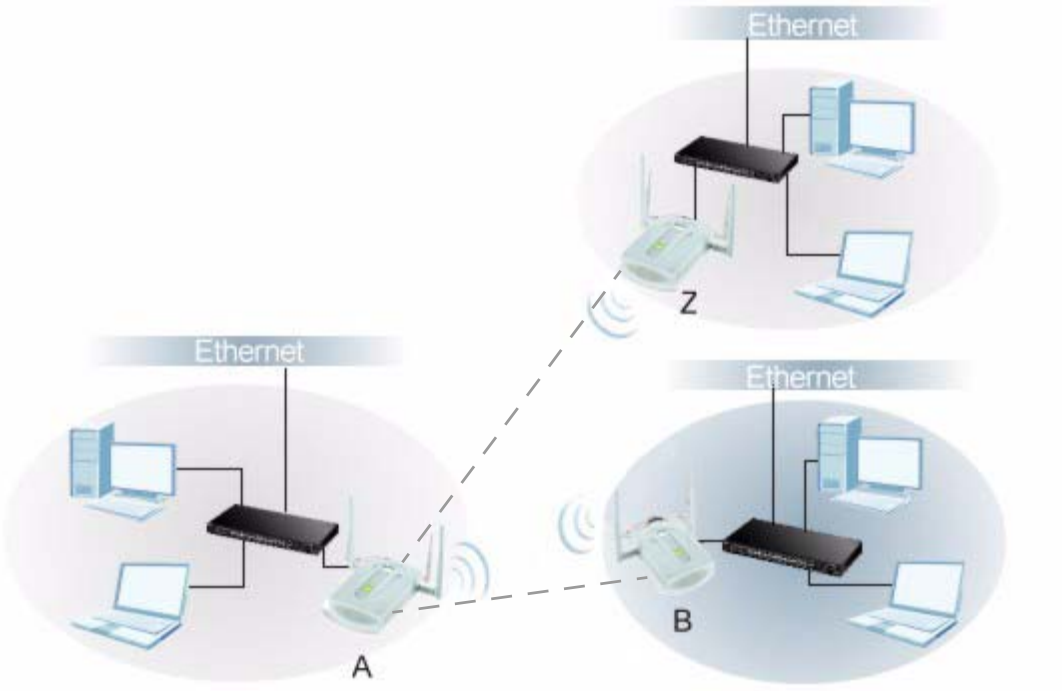
1.2.3 Bridge

The ZyXEL Device can act as a wireless network bridge and establish wireless links with other APs. In the figure below, the ZyXEL Devices (**A**, **B** and **Z**) are connected to independent wired networks and have a bridge connection (**A** can communicate with **B** and **Z**) at the same time. Security between bridged APs (the Wireless Distribution System or WDS) is independent of the security between the wired networks and their respective APs. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.3 on page 63 for more details.

Once the security settings of peer sides match one another, the connection between devices is made.

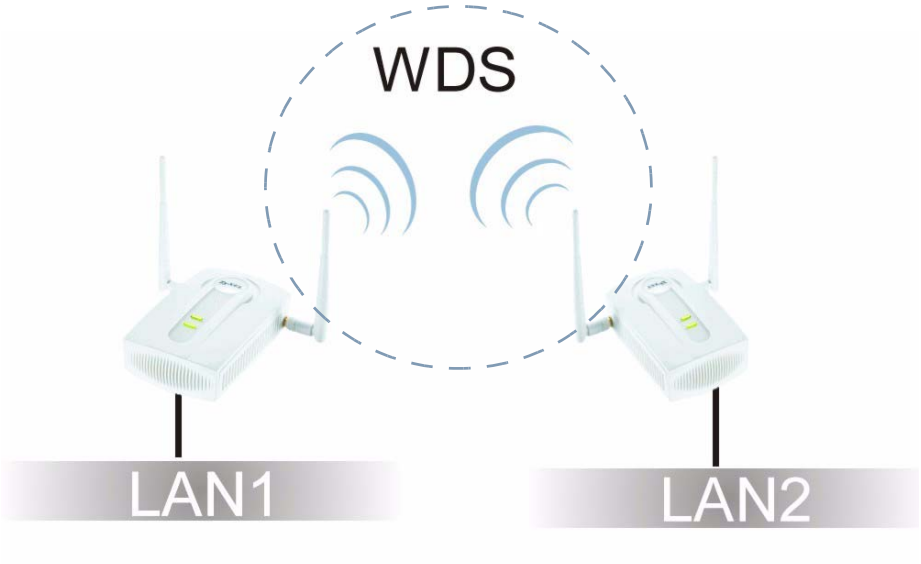
At the time of writing, WDS security is compatible with other ZyXEL NWA-series access points only. Refer to your other access point's documentation for details.

Figure 3 Bridge Application



In the example below, when both ZyXEL Devices are in Bridge mode, they form a WDS (Wireless Distribution System) allowing the computers in LAN 1 to connect to the computers in LAN 2.

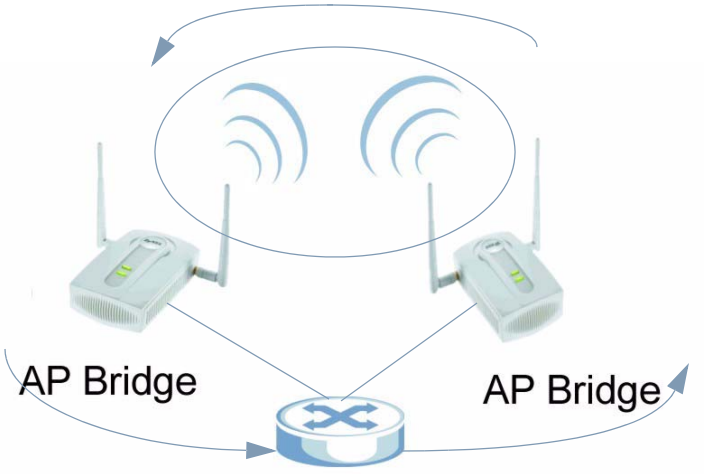
Figure 4 Bridging Example



Be careful to avoid bridge loops when you enable bridging in the ZyXEL Device. Bridge loops cause broadcast traffic to circle the network endlessly, resulting in possible throughput degradation and disruption of communications. The following examples show two network topologies that can lead to this problem:

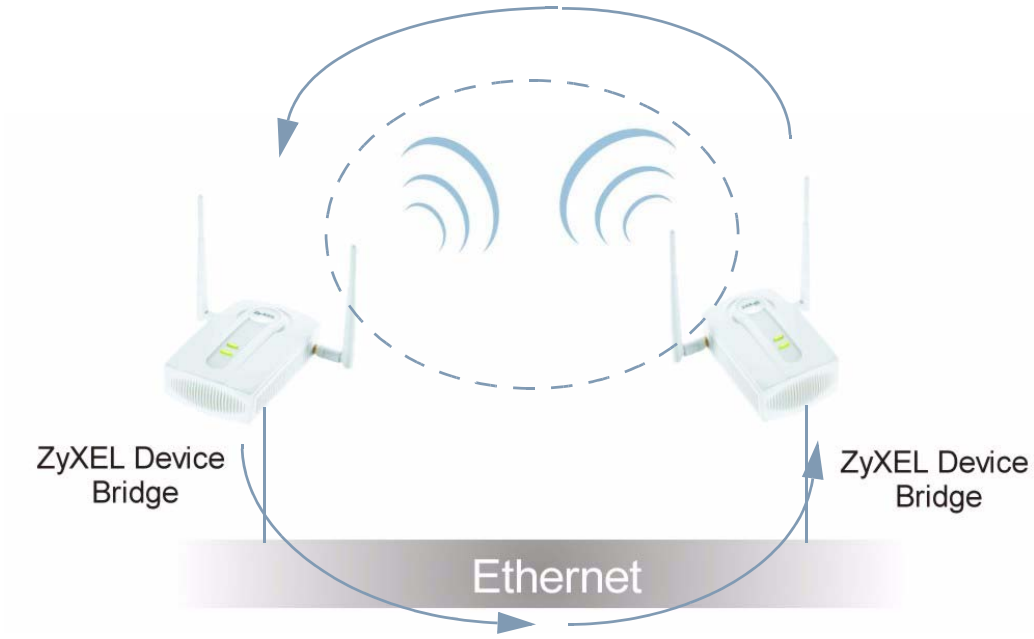
- If two or more ZyXEL Devices (in bridge mode) are connected to the same hub.

Figure 5 Bridge Loop: Two Bridges Connected to Hub



- If your ZyXEL Device (in bridge mode) is connected to a wired LAN while communicating with another wireless bridge that is also connected to the same wired LAN.

Figure 6 Bridge Loop: Bridge Connected to Wired LAN



To prevent bridge loops, ensure that you enable STP in the **Wireless** screen or your ZyXEL Device is not set to bridge mode while connected to both wired and wireless segments of the same LAN.

1.2.4 AP + Bridge

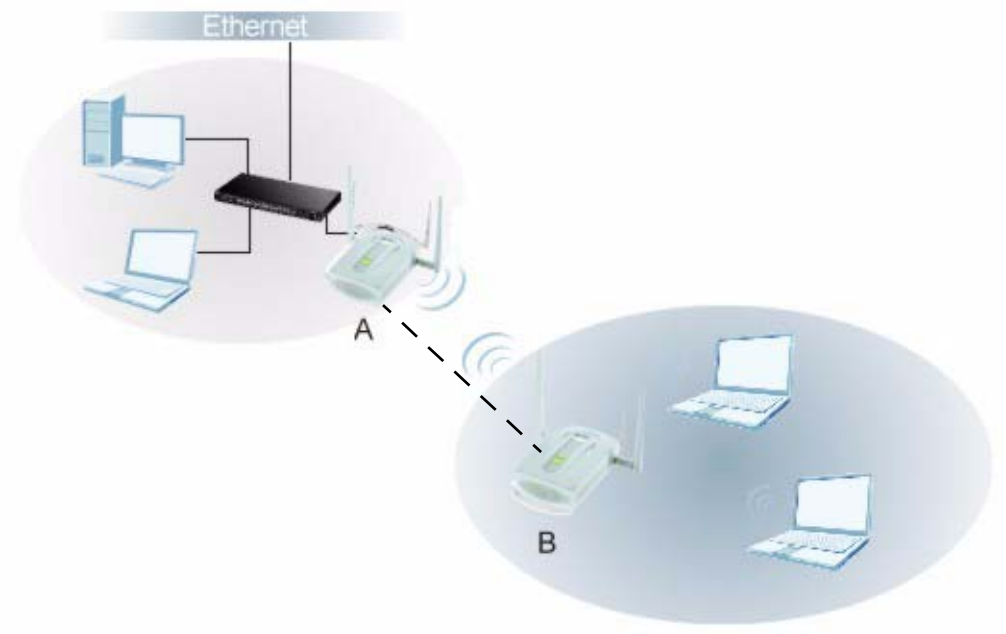
In **AP+Bridge** mode, the ZyXEL Device supports both AP and bridge connection at the same time.

Using AP + Bridge mode, your ZyXEL Device can extend the range of the WLAN. In the figure below, **A** and **B** act as AP + Bridge devices that forward traffic between associated wireless workstations and the wired LAN.

When the ZyXEL Device is in **AP+Bridge** mode, security between APs (the Wireless Distribution System or WDS) is independent of the security between the wireless stations and the AP. If you do not enable WDS security, traffic between APs is not encrypted. When WDS security is enabled, both APs must use the same pre-shared key. See Section 6.4.4 on page 67 for more details.

Unless specified, the term "security settings" refers to the traffic between the wireless stations and the ZyXEL Device.

Figure 7 AP + Bridge Application



1.3 Ways to Manage the ZyXEL Device

Use any of the following methods to manage the ZyXEL Device.

- Web Configurator. This is recommended for everyday management of the ZyXEL Device using a (supported) web browser.
- Command Line Interface. Line commands are mostly used for troubleshooting by service engineers.
- FTP (File Transfer Protocol) for firmware upgrades.
- SNMP (Simple Network Management Protocol). The device can be monitored by an SNMP manager.

1.4 Configuring Your ZyXEL Device's Security Features

Your ZyXEL Device comes with a variety of security features. This section summarizes these features and provides links to sections in the User's Guide to configure security settings on your ZyXEL Device. Follow the suggestions below to improve security on your ZyXEL Device and network.

1.4.1 Control Access to Your Device

Ensure only people with permission can access your ZyXEL Device.

- Control physical access by locating devices in secure areas, such as locked rooms. Most ZyXEL Devices have a reset button. If an unauthorized person has access to the reset button, they can then reset the device's password to its default password, log in and reconfigure its settings.
- Change any default passwords on the ZyXEL Device, such as the password used for accessing the ZyXEL Device's web configurator (if it has a web configurator). Use a password with a combination of letters and numbers and change your password regularly. Write down the password and put it in a safe place.
- Avoid setting a long timeout period before the ZyXEL Device's web configurator automatically times out. A short timeout reduces the risk of unauthorized person accessing the web configurator while it is left idle.
- See Chapter 5 on page 47 for instructions on changing your password and setting the timeout period.
- Configure remote management to control who can manage your ZyXEL Device. See Chapter 11 on page 101 for more information. If you enable remote management, ensure you have enabled remote management only on the IP addresses, services or interfaces you intended and that other remote management settings are disabled.

1.4.2 Wireless Security

Wireless devices are especially vulnerable to attack. If your ZyXEL Device has a wireless function, take the following measures to improve wireless security.

- Enable wireless security on your ZyXEL Device. Choose the most secure encryption method that all devices on your network support. See Section 7.4 on page 76 for directions on configuring encryption. If you have a RADIUS server, enable IEEE 802.1x or WPA(2) user identification on your network so users must log in. This method is more common in business environments.
- Hide your wireless network name (SSID). The SSID can be regularly broadcast and unauthorized users may use this information to access your network. See Section 6.4 on page 57 for directions on using the web configurator to hide the SSID.
- Enable the MAC filter to allow only trusted users to access your wireless network or deny unwanted users access based on their MAC address. See Section 9.4 on page 94 for directions on configuring the MAC filter.

1.5 Good Habits for Managing the ZyXEL Device

Do the following things regularly to make the ZyXEL Device more secure and to manage it more effectively.

1.6 Hardware Connections

See your Quick Start Guide for information on making hardware connections.

1.7 LEDs

Figure 8 LEDs

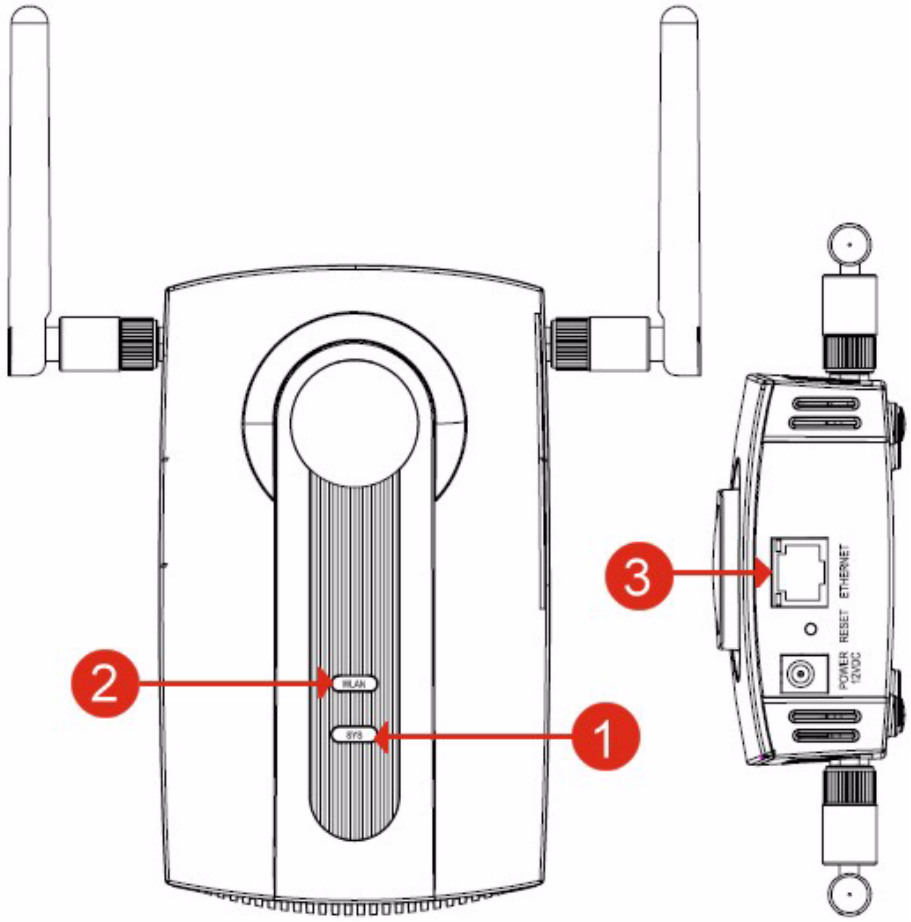


Table 1 LEDs

LABEL	LED	COLOR	STATUS	DESCRIPTION
1	SYS	Green	On	The ZyXEL Device is in AP + Bridge or Bridge mode, and has successfully established a Wireless Distribution System (WDS) connection.
		Amber	Flashing	The ZyXEL Device is starting up.
			Off	Either • The ZyXEL Device is in Access Point or mode and is functioning normally. • The ZyXEL Device is in AP+Bridge or Bridge mode and has not established a Wireless Distribution System (WDS) connection. or • The ZyXEL Device is not receiving power.
2	WLAN	Green	On	The wireless adaptor WLAN is active.
			Blinking	The wireless adaptor WLAN is active, and transmitting or receiving data.

Table 1 LEDs (continued)

LABEL	LED	COLOR	STATUS	DESCRIPTION
			Off	The wireless adaptor WLAN is not active.
3	ETHERNET	Green	On	The ZyXEL Device has a 10 Mbps Ethernet connection.
			Blinking	The ZyXEL Device has a 10 Mbps Ethernet connection and is sending or receiving data.
		Yellow	On	The ZyXEL Device has a 100 Mbps Ethernet connection.
			Blinking	The ZyXEL Device has a 100 Mbps Ethernet connection and is sending/receiving data.
			Off	The ZyXEL Device does not have an Ethernet connection.

2

Introducing the Web Configurator

This chapter describes how to access the ZyXEL Device's web configurator and provides an overview of its screens.

2.1 Accessing the Web Configurator

1. Make sure your hardware is properly connected and prepare your computer or computer network to connect to the ZyXEL Device (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "192.168.1.2" as the URL (default).
4. Type "1234" (default) as the password and click **Login**. In some versions, the default password appears automatically - if this is the case, click **Login**.
5. You should see a screen asking you to change your password (highly recommended) as shown next. Type a new password (and retype it to confirm) then click **Apply**. Alternatively, click **Ignore**.

Note: If you do not change the password, the following screen appears every time you login.

Figure 9 Change Password Screen

You should now see the **Status** screen. See Chapter 2 on page 29 for details about the **Status** screen.

Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back into the ZyXEL Device if this happens.

2.2 Resetting the ZyXEL Device

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button. This replaces the current configuration file with the factory-default configuration file. This means that you will lose all the settings you previously configured. The password will be reset to 1234.

2.2.1 Methods of Restoring Factory-Defaults

You can erase the current configuration and restore factory defaults in two ways:

Use the **RESET** button to upload the default configuration file. Hold this button in for about 10 seconds (the lights will begin to blink). Use this method for cases when the password or IP address of the ZyXEL Device is not known.

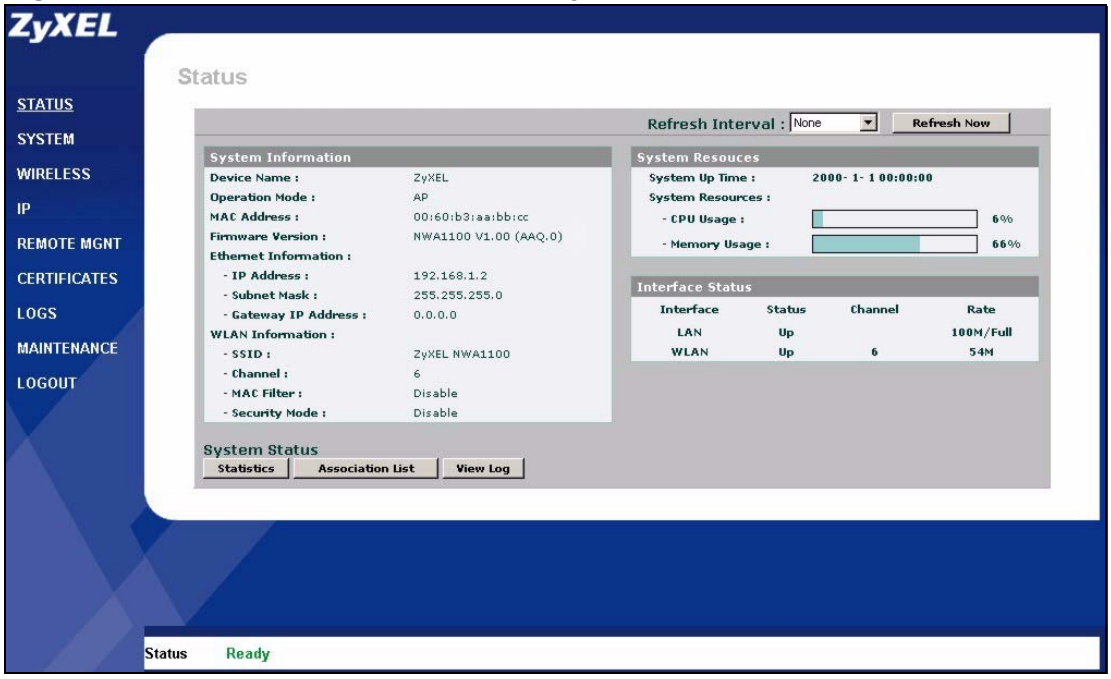
Use the web configurator to restore defaults (refer to Section 14.7 on page 127).

2.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **Status** screen.

Check the status bar at the bottom of the screen when you click **Apply** or **OK** to verify that the configuration has been updated.

Figure 10 Status Screen of the Web Configurator



- Click the links on the left of the screen to configure advanced features such as **SYSTEM** (General, Password and Time), **WIRELESS** (Wireless Settings, Security, RADIUS, MAC Filter), **IP**, **REMOTE MGNT** (Telnet, FTP, WWW and SNMP), **CERTIFICATES**, and **LOGS** (View Log and Log Settings).
- Click **MAINTENANCE** to view information about your ZyXEL Device or upgrade configuration and firmware files. Maintenance features include **Association List**, **Channel Usage**, **F/W** (firmware) **Upload**, **Configuration File** (Backup, Restore and Default) and **Restart**.
- Click **LOGOUT** at any time to exit the web configurator.

3

Status Screens

The **Status** screens display when you log into the ZyXEL Device, or click **Status** in the navigation menu.

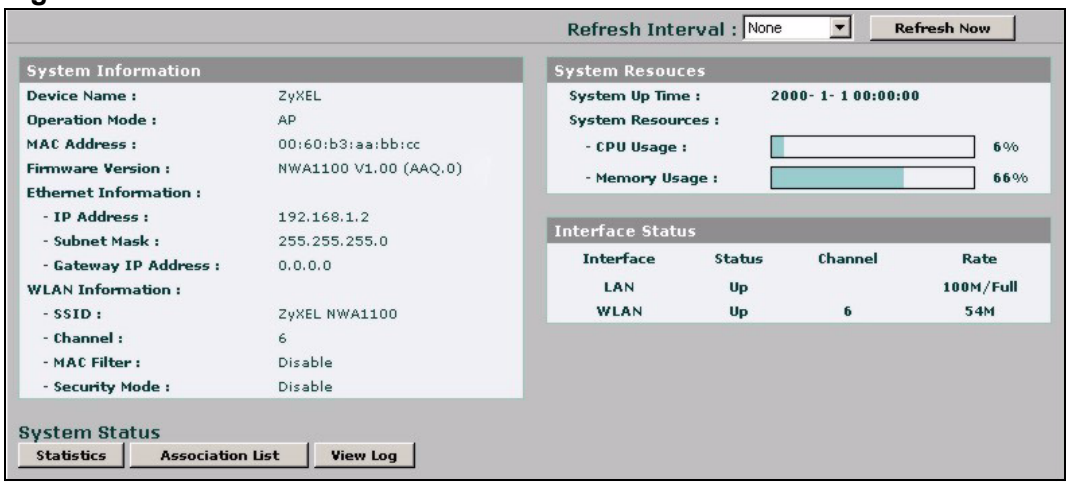
Use the **Status** screens to look at the current status of the device, system resources, and interfaces. The **Status** screens also provide detailed information about system statistics, associated wireless clients, and logs.

3.1 The Status Screen

Use this screen to get a quick view of system, Ethernet, WLAN and other information regarding your ZyXEL Device.

Click **Status**. The following screen displays.

Figure 11 The Status Screen



The following table describes the labels in this screen.

Table 2 The Status Screen

LABEL	DESCRIPTION
Refresh Interval	Enter how often you want the ZyXEL Device to update this screen.
Refresh Now	Click this to update this screen immediately.
System Information	
Device Name	This field displays the ZyXEL Device system name. It is used for identification. You can change this in the **System > General** screen's **Device Name** field.
Operation Mode	This field displays the current operating mode of the first wireless module (**AP**, **Wireless Client**, **Bridge or AP+Bridge**). You can change the operating mode in the **Wireless** > **Wireless Settings** screen.
MAC Address	This displays the MAC (Media Access Control) address of the ZyXEL Device on the LAN. Every network device has a unique MAC address which identifies it across the network.
Firmware Version	This field displays the current version of the firmware inside the device. It also shows the date the firmware version was created. You can change the firmware version by uploading new firmware in **Maintenance > F/W Upload**.
Ethernet Information	
IP Address	This field displays the current IP address of the ZyXEL Device on the network.
Subnet Mask	Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.
Gateway IP Address	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN port. The gateway helps forward packets to their destinations.
WLAN Information	
SSID	This field displays the SSID (Service Set Identifier).
Channel	The channel or frequency used by the ZyXEL Device to send and receive information.
MAC Filter	Media Access Control filtering checks incoming frames based on MAC (Media Access Control) address(es) that you specify.
Security Mode	This displays the security mode the ZyXEL Device is using.
System Resources	
System Up Time	This field displays the elapsed time since the ZyXEL Device was turned on.
CPU Usage	This field displays what percentage of the ZyXEL Device's processing ability is currently being used. The higher the CPU usage, the more likely the ZyXEL Device is to slow down.
Memory Usage	This field displays what percentage of the ZyXEL Device's volatile memory is currently in use. The higher the memory usage, the more likely the ZyXEL Device is to slow down. Some memory is required just to start the ZyXEL Device and to run the web configurator.

Table 2 The Status Screen

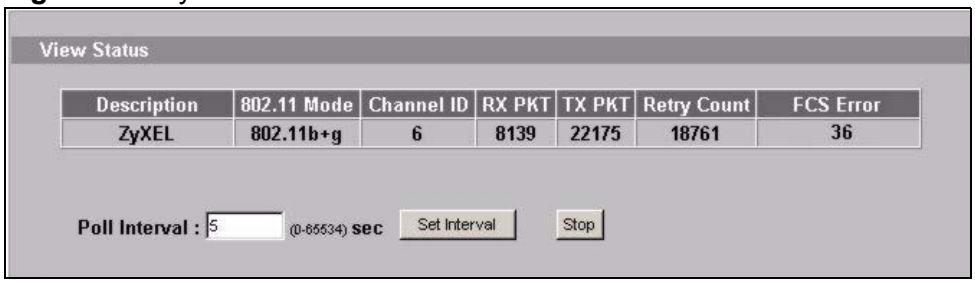
LABEL	DESCRIPTION
Interface Status	
Interface	This column displays each interface of the ZyXEL Device.
Status	This field indicates whether or not the ZyXEL Device is using the interface. For each interface, this field displays **Up** when the ZyXEL Device is using the interface and **Down** when the ZyXEL Device is not using the interface.
Channel	Click this to see which wireless channels are currently in use in the local area. See Section 14.5 on page 124.
Rate	For the LAN port this displays the port speed and duplex setting. For the WLAN interface, it displays the downstream and upstream transmission rate or **N/A** if the interface is not in use.
LAN	This field displays the number of wireless clients currently associated to the first wireless module. Each wireless module supports up to 32 concurrent associations.
WLAN	This field displays the number of wireless clients currently associated to the second wireless module. Each wireless module supports up to 32 concurrent associations.
System Status	
Statistics	Click this link to view port status and packet specific statistics. See Section 3.1.1 on page 35.
Association List	Click this to see a list of wireless clients currently associated to each of the ZyXEL Device's wireless modules. See Section 14.4 on page 124.
View Log	Click this to see a list of logs produced by the ZyXEL Device. See Chapter 13 on page 115.

3.1.1 System Statistics Screen

Use this screen to view read-only information, including 802.11 Mode, Channel ID, Retry Count and FCS Error Count. Also provided is the "poll interval". The **Poll Interval** field is configurable. The fields in this screen vary according to the current wireless mode of each WLAN adaptor.

Click **Status > Show Statistics**. The following screen pops up.

Figure 12 System Status: Show Statistics



The following table describes the labels in this screen.

Table 3 System Status: Show Statistics

LABEL	DESCRIPTION
Description	
802.11 Mode	This field shows which mode (802.11b Only, 802.11g Only, 802.11b+g) the ZyXEL Device is using.
Channel ID	Click this to see which wireless channels are currently in use in the local area. See Section 14.5 on page 124.
RX PKT	This is the number of received packets on this port.
TX PKT	This is the number of transmitted packets on this port.
Retry Count	This is the total number of retries for transmitted packets (TX).
FCS Error	This is the ratio percentage showing the total number of checksum error of received packets (RX) over total RX.

4

Tutorial

This chapter first provides an overview of how to configure the wireless LAN on your ZyXEL Device, and then gives step-by-step guidelines showing how to configure your ZyXEL Device for some example scenarios.

4.1 How to Configure the Wireless LAN

This section illustrates how to choose which wireless operating mode to use on the ZyXEL Device and how to set up the wireless LAN in each wireless mode. See Section 4.1.3 on page 38 for links to more information on each step.

4.1.1 Choosing the Wireless Mode

- Use **Access Point** operating mode if you want to allow wireless clients to access your wired network, all using the same security and Quality of Service (QoS) settings. See Section 1.2.1 on page 20 for details.
- Use **Wireless Client** operating mode if you want to use the ZyXEL Device to access a wireless network. See Section 1.2.2 on page 21 for details.
- Use **Bridge** operating mode if you want to use the ZyXEL Device to communicate with other access points. See Section 1.2.3 on page 21 for details.

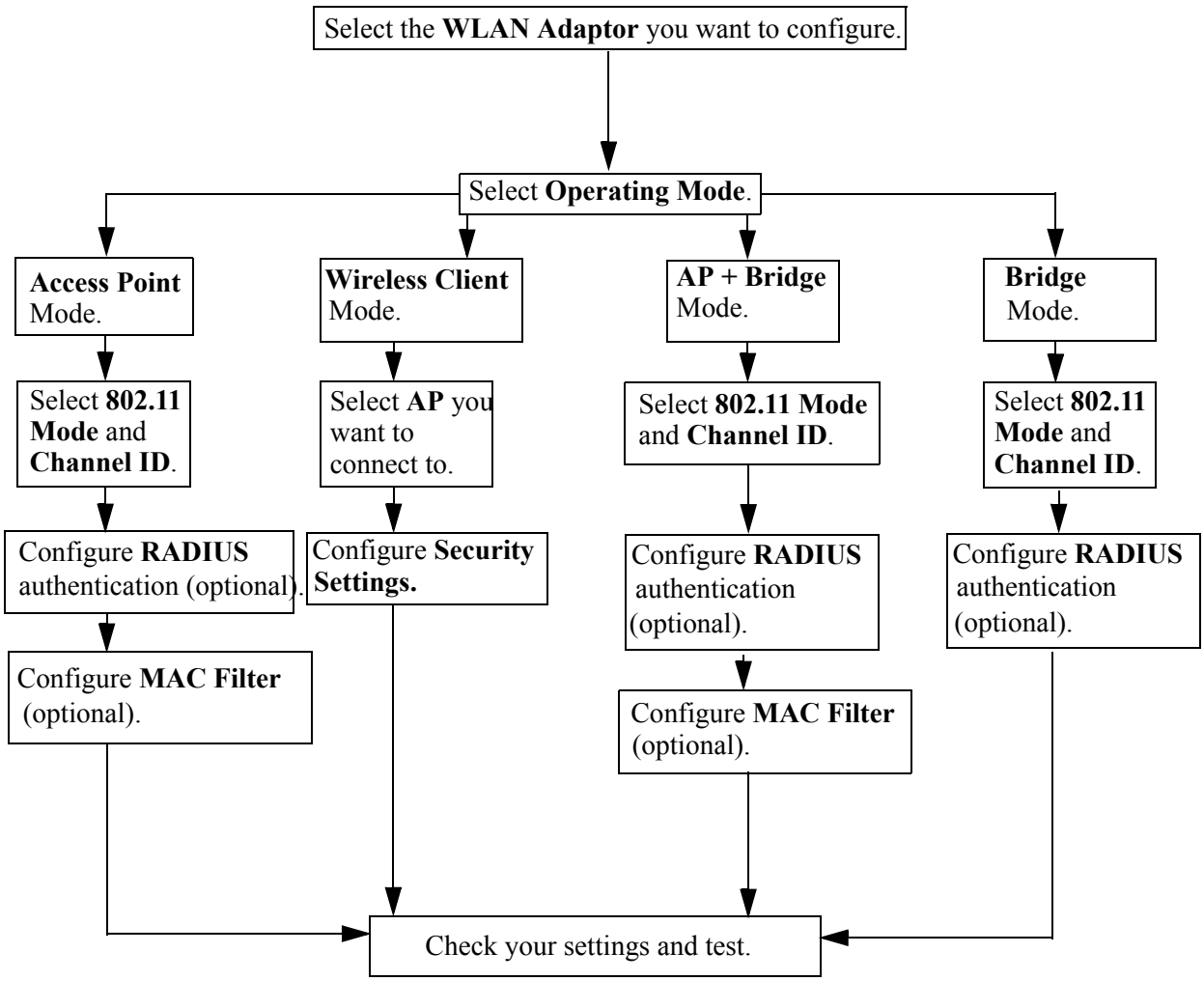
  The ZyXEL Device is a bridge when other APs access your wired Ethernet network through the ZyXEL Device.
- Use **AP + Bridge** operating mode if you want to use the ZyXEL Device as an access point (see above) while also communicating with other access points. See Section 1.2.4 on page 24 for details.

4.1.2 Wireless LAN Configuration Overview

The following figure shows the steps you should take to configure the wireless settings according to the operating mode you select. Use the Web Configurator to set up your ZyXEL Device's wireless network (see your Quick Start Guide for

information on setting up your ZyXEL Device and accessing the Web Configurator).

Figure 13 Configuring Wireless LAN


Select the **WLAN Adaptor** you want to configure.
Select **Operating Mode**.
Access Point Mode.
Wireless Client Mode.
AP + Bridge Mode.
Bridge Mode.
Select **802.11 Mode** and **Channel ID**.
Select **AP** you want to connect to.
Select **802.11 Mode** and **Channel ID**.
Select **802.11 Mode** and **Channel ID**.
Configure **RADIUS** authentication (optional).
Configure **Security Settings.**
Configure **RADIUS** authentication (optional).
Configure **RADIUS** authentication (optional).
Configure **MAC Filter** (optional).
Configure **MAC Filter** (optional).
Check your settings and test.

4.1.3 Further Reading

Use these links to find more information on the steps:

- Selecting a **WLAN Adaptor**: see Section 6.4.1 on page 58.
- Choosing **802.11 Mode**: see Section 6.4.1 on page 58.
- Choosing a wireless **Channel ID**: see Section 6.4.1 on page 58.
- Choosing a **Security** mode: see Section 7.4.1 on page 77.
- Configuring an external **RADIUS** server: see Section 8.4 on page 90.
- Configuring **MAC Filtering**: see Section 9.1 on page 93.

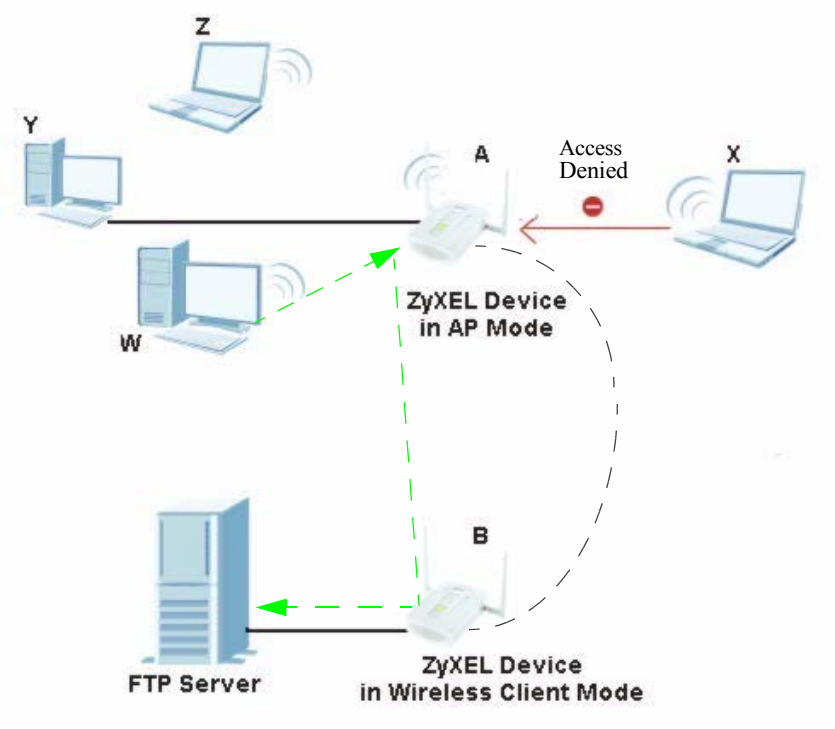
4.2 ZyXEL Device Setup in Wireless Client Mode

This example shows you how to restrict wireless access to your ZyXEL Device.

4.2.1 Scenario

In the figure below, there are two ZyXEL Devices (**A** and **B**) in the network. **A** is in Access Point (AP) mode while **B** is in Wireless Client mode. Station **B** is connected to a File Transfer Protocol (FTP) server. You want only specified wireless clients to be able to access station **B**. You also want to allow wireless traffic between **B** and wireless clients connected to **A** (**W, Y** and **Z**). Other wireless devices (**X**) must not be able to connect to the FTP server.

Figure 14 FTP Server Connected to a Wireless Client

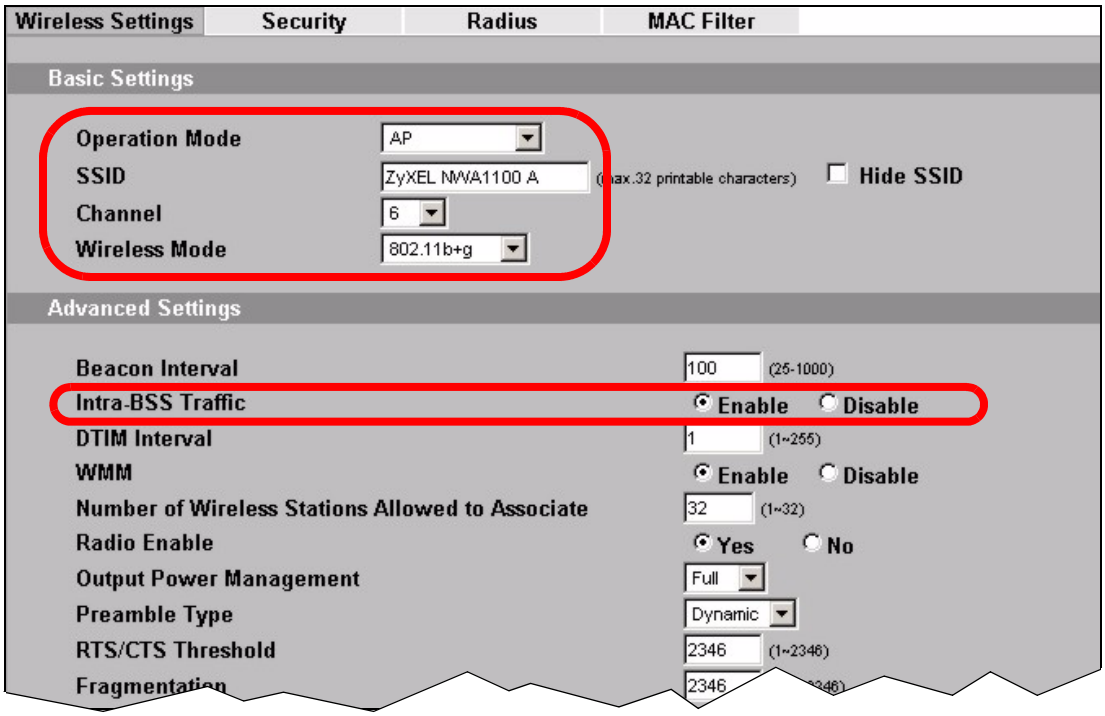


4.2.2 Configuring the ZyXEL Device in Access Point Mode

Before setting up the ZyXEL Device as a wireless client (**B**), you need to make sure there is an access point to connect to. Use the Ethernet port on your ZyXEL Device to configure it via a wired connection.

Open the Web Configurator and go to the **Wireless > Wireless Settings** screen.

Figure 15 Access Point Mode Wireless Setttings



1 Set the **Operation Mode** to **AP**.

2 Enter an **SSID** name, such as "NWA-1100 A".

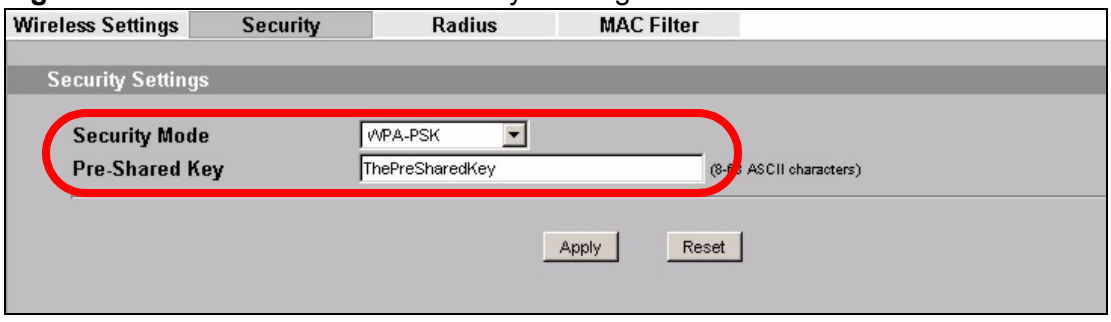
3 Choose the channel you want the ZyXEL Device to use.

4 Select the **Wireless Mode**.

5 Set the **Intra-BSS Traffic** to **Enable**.

6 Go to **Wireless > Security** to configure the ZyXEL Device to use WPA-PSK security mode.

Figure 16 Access Point Mode Security Setttings



4.2.3 Configuring the ZyXEL Device in Wireless Client Mode

Your ZyXEL Device should have a wired connection before it can be set to wireless client operating mode. Connect your ZyXEL Device to the FTP server. Open the Web Configurator ZyXEL Device and go to the **Wireless > Wireless Settings** screen. Follow these steps to configure Station **B**.

1. Select **Wireless Client** as **Operating Mode**. Wait for the screen to refresh.
2. You should now see a tab that says **Site Survey** (refer to Figure 18). Click on this. A window should pop up which contains a list of all available wireless devices within your ZyXEL Device's range. Copy the SSID of the AP you want your wireless client to connect to (refer to Figure 19).
3. For this example, you want to connect to the access point, **A**.The SSID that you should copy is **ZyXEL NWA-1100 A** (refer to Figure 15 to check the SSID of Station **A**).
4. Go back to the screen in Figure 17. In the **SSID** field, enter **ZyXEL NWA-1100 A** (refer to Figure 18).

5 Set the **Wireless Mode** to the same one set for the access point. **Click Apply**.

Figure 17 Wireless Client Mode Wireless Settings

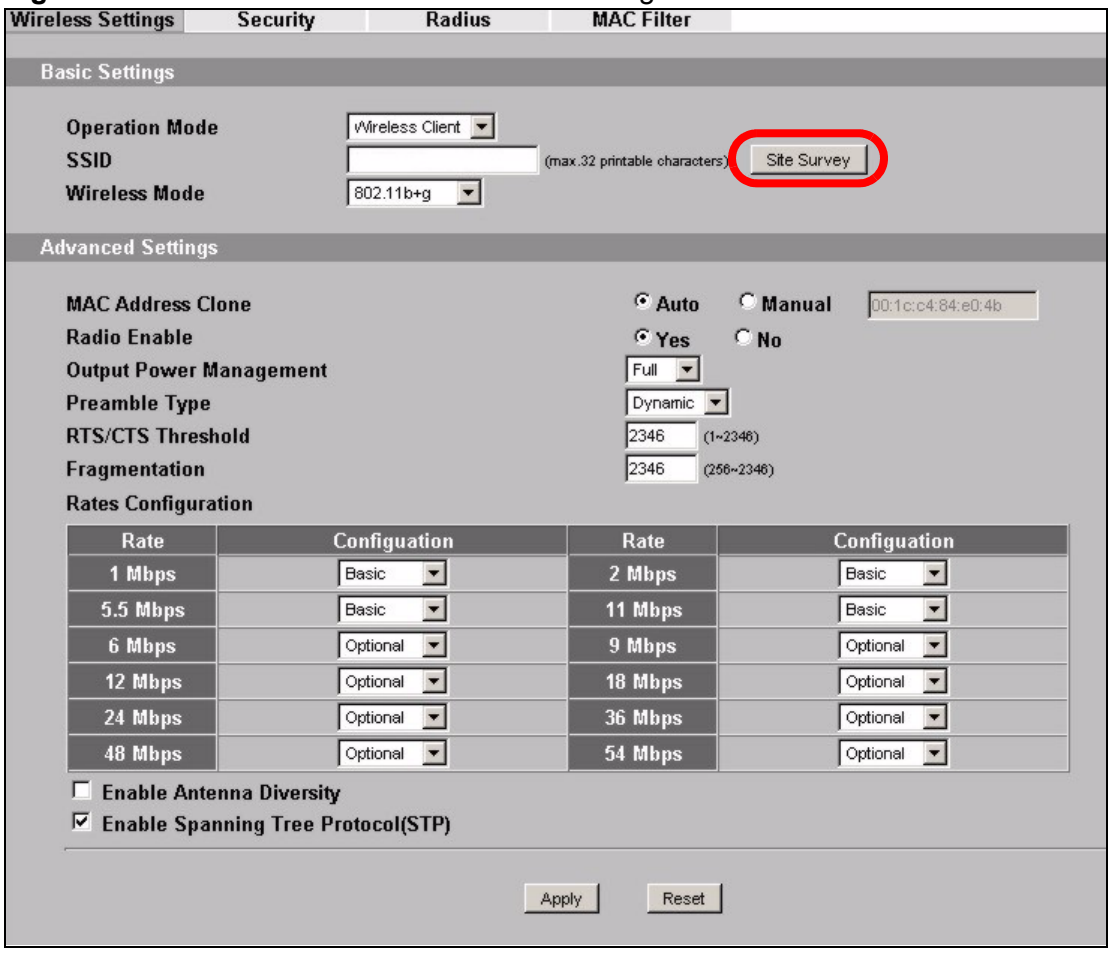
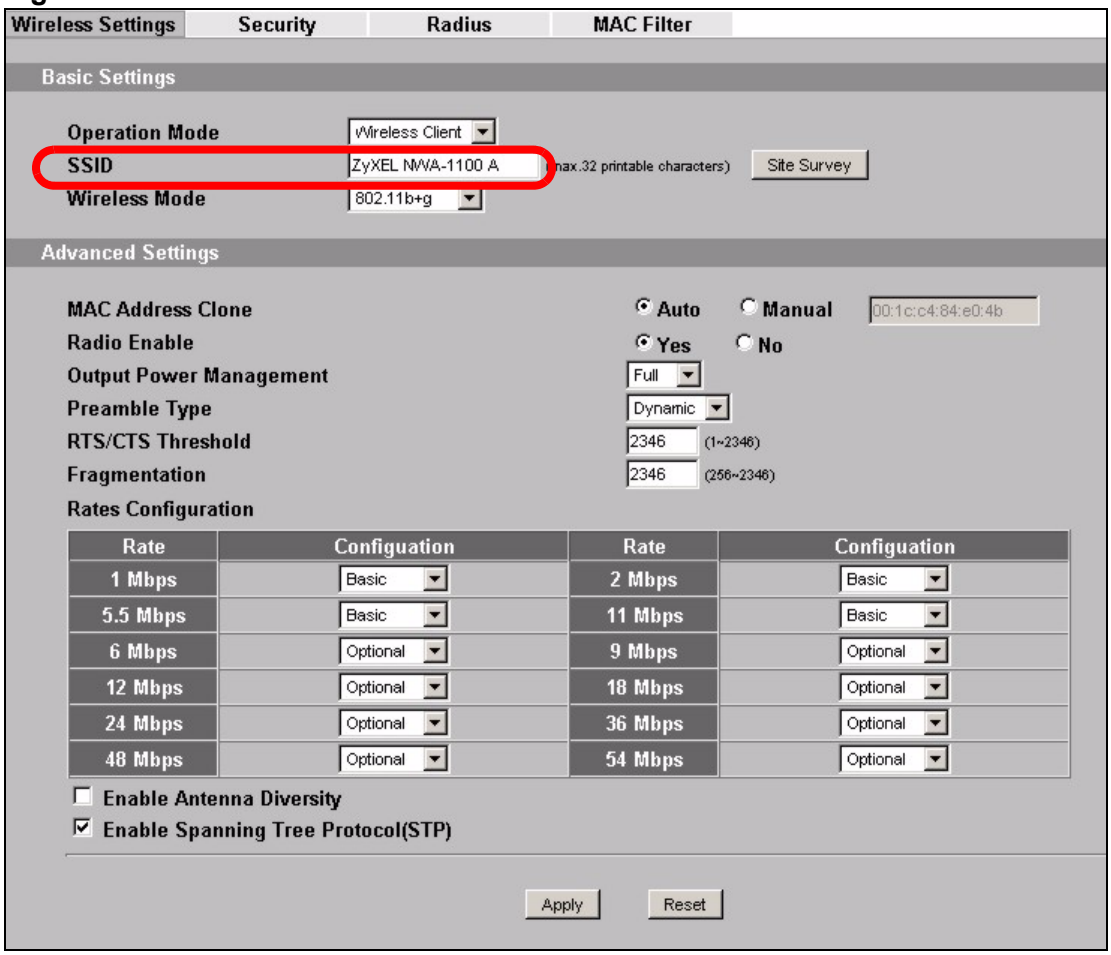


Figure 18 Site Survey

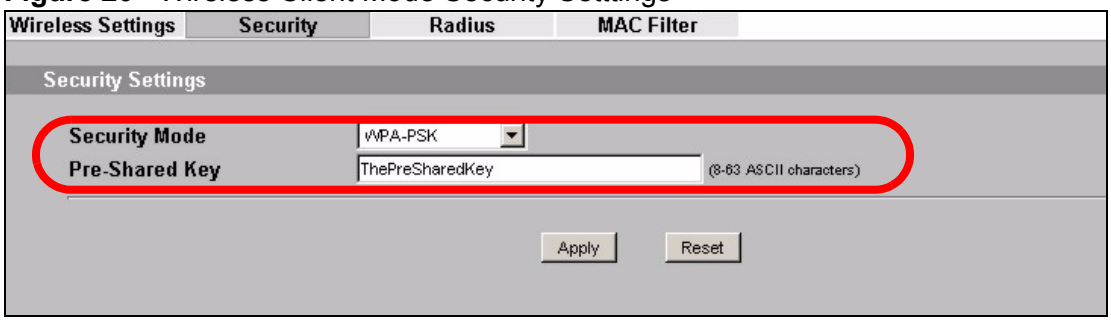
SSID	BSSID	Channel	Wireless Mode	Security	Signal Strength
ZyXEL NWA-1100 A	06:13:49:DF:42:A8	6	802.11g only	none	90%

Figure 19 Wireless Client Mode



6 Go to **Wireless > Security** to configure the ZyXEL Device to use WPA-PSK security mode.

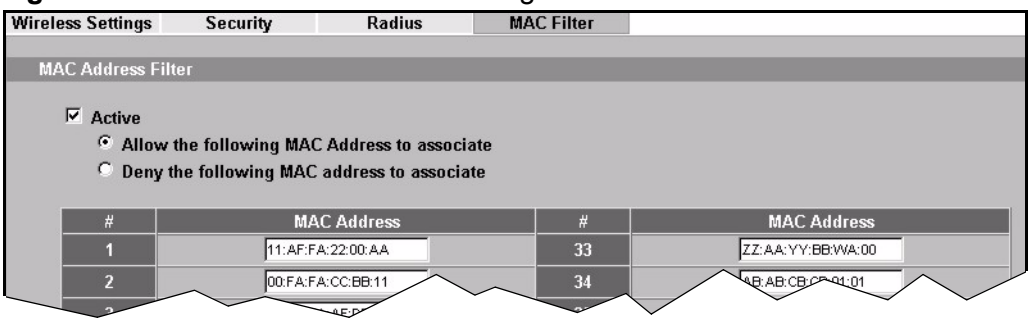
Figure 20 Wireless Client Mode Security Setttings



7 One way to ensure that only specified wireless clients can access the FTP server is by enabling MAC filtering on the ZyXEL Device. See Chapter 9 on page 93 for more information on the MAC Filter screen.

8 Still in the Web Configurator, go to **Wireless > MAC Filter**. Click on **Active** then highlight **Allow the following MAC Address to associate**. Enter the MAC Addresses of the wireless clients (**W, Y** and **Z**) you want to associate with the ZyXEL Device. Click **Apply**.

Figure 21 Wireless Client MAC Filtering



After following this tutorial, you should now have the same setup as shown in Figure 14.

4.2.4 Testing the Connection and Troubleshooting

This section discusses how you can check if you have correctly configured your network setup as described in this tutorial.

- Try accessing the FTP server from wireless clients **W, Y** or **Z**. Test if you can send or retrieve a file. If you cannot establish a connection with the FTP server, do the following steps.

1 Make sure **W, Y** and **Z** use the same wireless security settings as **A** and can access **A**.

2 Make sure **B** uses the same wireless and wireless security settings as **A** and can access **A**.

3 Make sure intra-BSS traffic is enabled on **A**.

- Try accessing the FTP server from **X**. If you are able to access the FTP server, do the following.

1 Make sure MAC filtering is enabled.

2 Make sure **X**'s MAC address is not entered in the list of allowed devices.

PART II
The Web Configurator

System Screens (47)

Wireless Settings Screen (55)

Wireless Security Screen (73)

RADIUS Screen (89)

MAC Filter Screen (93)

IP Screen (97)

Remote Management (101)

Certificate Screen (111)

Log Screens (115)

Maintenance (123)

Troubleshooting (131)

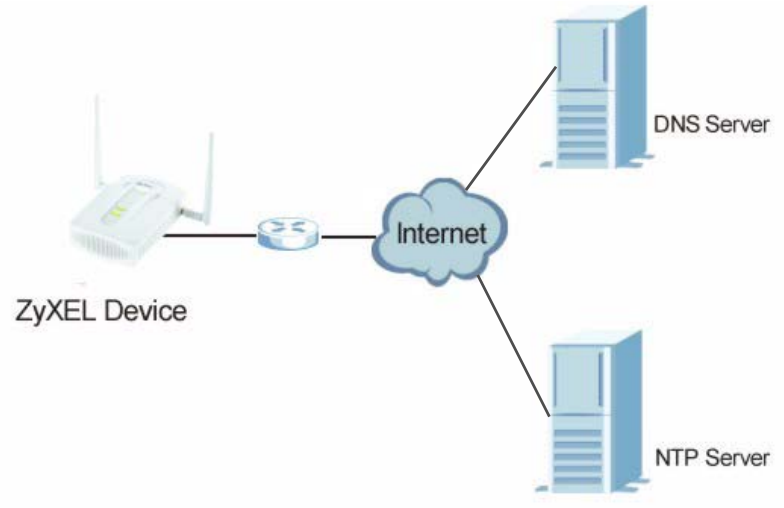
5

System Screens

5.1 Overview

This chapter provides information and instructions on how to identify and manage your ZyXEL Device over the network.

Figure 22 ZyXEL Device Setup



In the figure above, the ZyXEL Device connects to a Domain Name Server (DNS) server to avail of a domain name. It also connects to an Network Time Protocol (NTP) server to set the time on the device.

5.2 What You Can Do in the System Screens

- Use the **System > General** screen (see Section on page 49) to specify the **Device name** and **Administrator Inactivity Timer** value. You can also configure your **System DNS Servers** in this screen.
- Use the **System > Password** screen (see Section 5.4.1 on page 50) to manage the password for your ZyXEL Device.
- Use the **System > Time Setting** screen (see Section 5.5 on page 51) to change your ZyXEL Device's time and date. This screen allows you to configure the ZyXEL Device's time based on your local time zone.

5.3 What You Need To Know About the System Screens

IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet, for instance, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 4 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three

numbers specify the network number while the last number identifies an individual computer on that network.

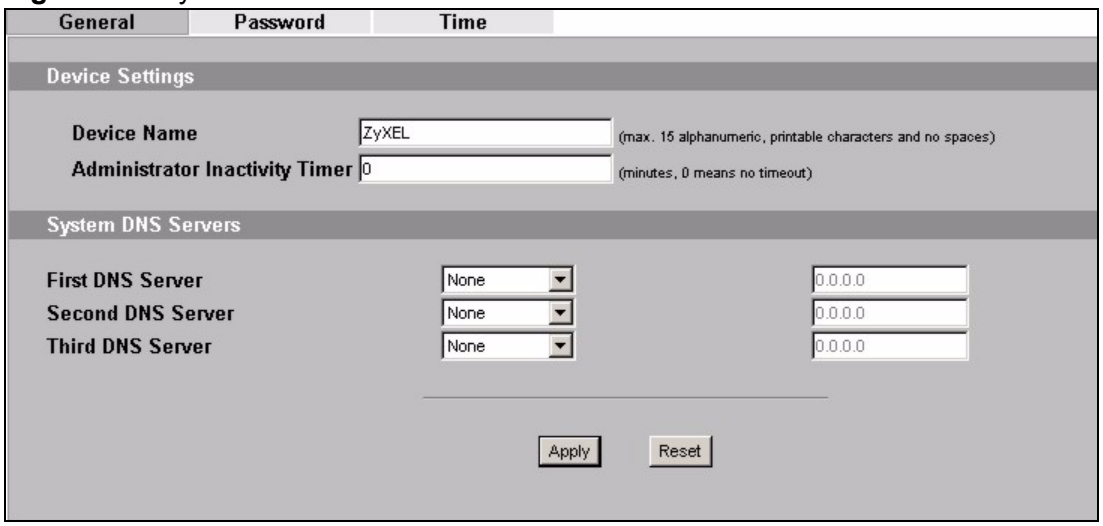
Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.2, for your device, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your device will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the device unless you are instructed to do otherwise.

5.4 General Screen

Use the General screen to identify your ZyXEL Device over the network. Click **System** > **General**. The following screen displays.

Figure 23 System: General



The following table describes the labels in this screen.

Table 5 System: General

LABEL	DESCRIPTION
Device Settings	
Device Name	Type a descriptive name to identify the ZyXEL Device in the Ethernet network. This name can be up to 15 alphanumeric characters long. Spaces are not allowed, but dashes "-" are accepted.

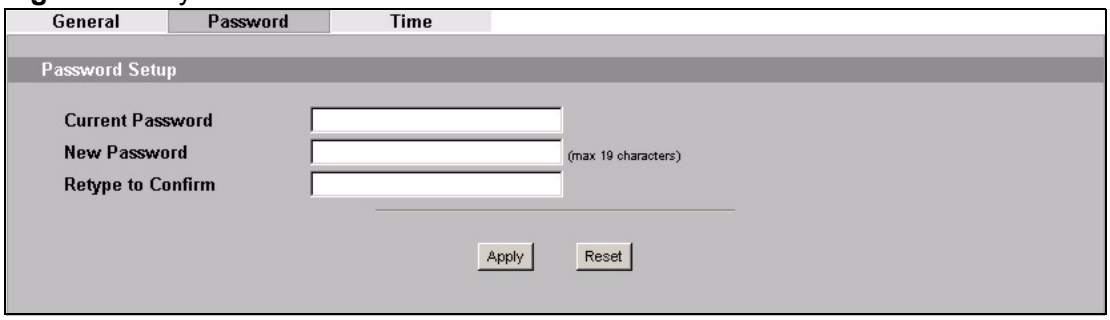
Table 5 System: General

LABEL	DESCRIPTION
Administrator Inactivity Timer	Type how many minutes a management session (via web configurator) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
System DNS Servers	
First DNS Server Second DNS Server Third DNS Server	The field to the right displays the (read-only) DNS server IP address that the DHCP assigns. Select **User-Defined** if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right. Select **None** if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it. The default setting is **None**.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.4.1 Password Screen

Use this screen to control access to your ZyXEL Device by assigning a password to it. Click **System > Password**. The following screen displays.

Figure 24 System: Password.



The following table describes the labels in this screen.

Table 6 System: Password

LABEL	DESCRIPTIONS
Current Password	Type in your existing system password ("1234" is the default password).
New Password	Type your new system password (max 19 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.

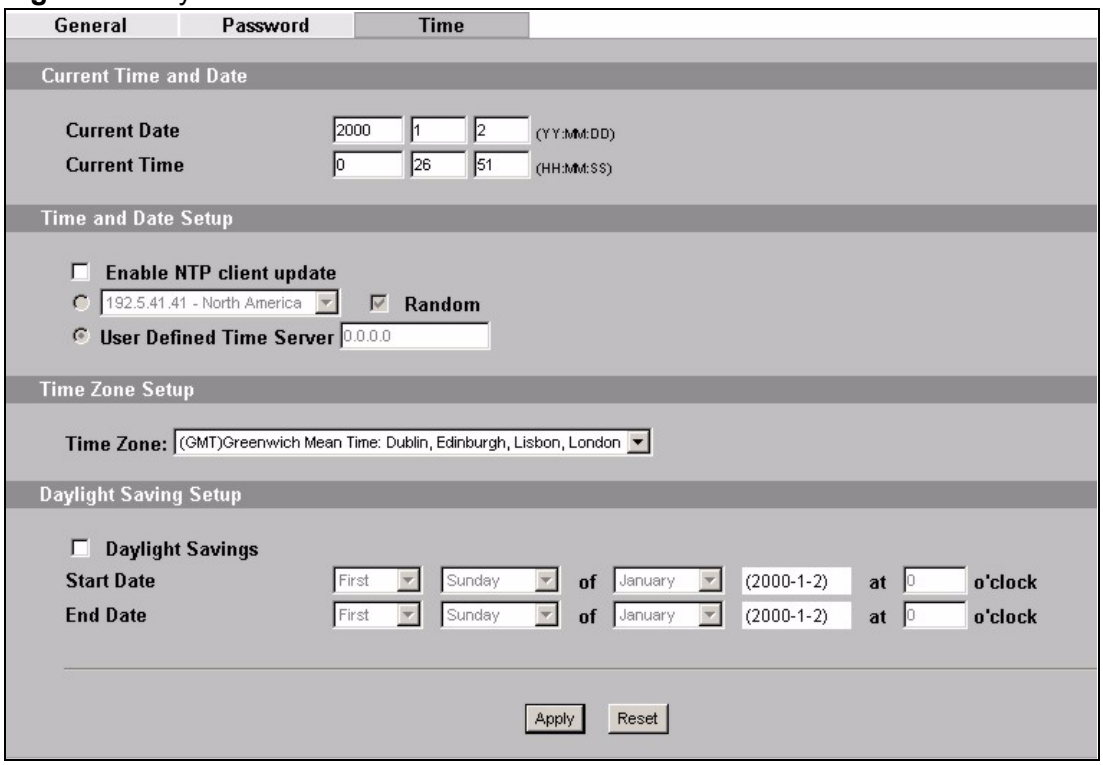
Table 6 System: Password

LABEL	DESCRIPTIONS
Retype to Confirm	Retype your new system password for confirmation.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.5 Time Screen

Use this screen to change your ZyXEL Device's time and date, click **System** > **Time**. The following screen displays.

Figure 25 System: Time



The following table describes the labels in this screen.

Table 7 System: Time

LABEL	DESCRIPTION
Current Time and Date	
Current Date	This field displays the last updated date from the time server.
Current Time	This field displays the time of your ZyXEL Device. Each time you reload this page, the ZyXEL Device synchronizes the time with the time server (if configured).
Time and Date Setup	

Table 7 System: Time

LABEL	DESCRIPTION
Enable NTP client update	Select this to have the ZyXEL Device use the predefined list of Network Time Protocol (NTP) servers.
Random	Select this to have the ZyXEL Device select which NTP server to use.
User Defined Time Server	Enter the IP address or URL of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Saving Setup	
Daylight Savings	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Enable Daylight Saving**. The **at** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **Second**, **Sunday**, **March** and **2:00**. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **March**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type **2** because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Enable Daylight Saving**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **First**, **Sunday**, **November** and **2:00**. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **Last**, **Sunday**, **October**. The time you type in the **at** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to reload the previous configuration for this screen.

5.6 Technical Reference

This section provides some technical information about the topics covered in this chapter.

5.6.1 Pre-defined NTP Time Servers List

When you turn on the ZyXEL Device for the first time, the date and time start at 2000-01-01 00:00:00. When you select **Auto** in the **System** > **Time Setting** screen, the ZyXEL Device then attempts to synchronize with one of the following pre-defined list of NTP time servers.

The ZyXEL Device continues to use the following pre-defined list of NTP time servers if you do not specify a time server or it cannot synchronize with the time server you specified.

Table 8 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

When the ZyXEL Device uses the pre-defined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the ZyXEL Device goes through the rest of the list in order from the first one tried until either it is successful or all the pre-defined NTP time servers have been tried.

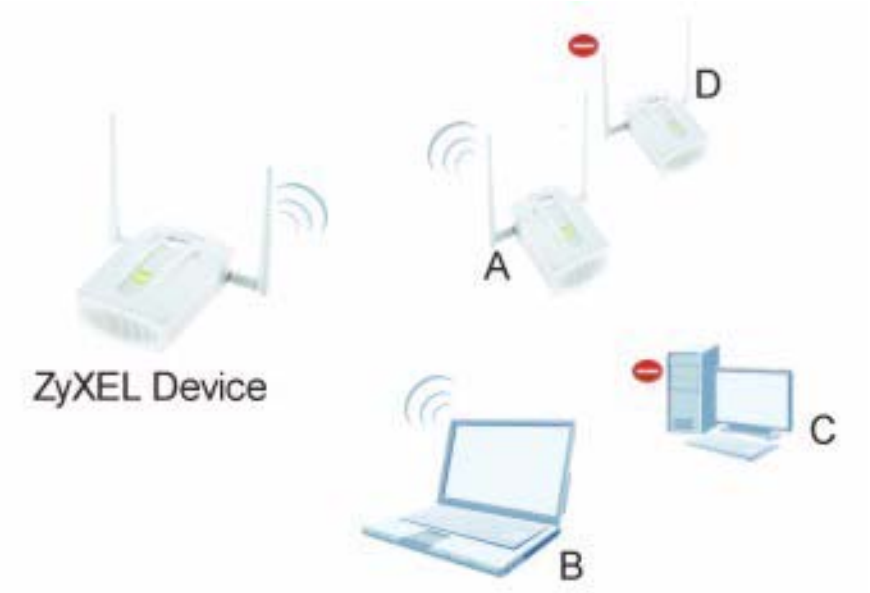
6

Wireless Settings Screen

6.1 Overview

This chapter discusses the steps to configure the Wireless Settings screen on the ZyXEL Device. It also introduces the wireless LAN (WLAN) and some basic scenarios.

Figure 26 Wireless Mode



In the figure above, the ZyXEL Device allows access to another bridge device (A) and a notebook computer (B) upon verifying their settings and credentials. It denies access to other devices (C and D) with configurations that do not match those specified in your ZyXEL Device.

6.2 What You Can Do in the Wireless Settings Screen

Use the **Wireless > Wireless Settings** screen (see Section 6.4 on page 57) to configure the ZyXEL Device to operate in AP (Access Point), Wireless Client, Bridge or AP + Bridge.

6.3 What You Need To Know About Wireless Settings Screen

BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Intra-BSS traffic is traffic between wireless clients in the BSS.

ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

Operating Mode

The ZyXEL Device can run in four operating modes as follows:

- **AP (Access Point)**. The ZyXEL Device is wireless access point that allows wireless communication to other devices in the network.
- **Wireless Client.** The ZyXEL Device acts as a wireless client to access a wireless network.
- **Bridge.** The ZyXEL Device acts as a wireless network bridge and establishes wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode. The ZyXEL Device can establish up to five wireless links with other APs.
- **AP+Bridge Mode.** The ZyXEL Device functions as a bridge and access point simultaneously.

Refer to Chapter 1 on page 19 for illustrations of these wireless applications.

SSID

The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID.

Normally, the ZyXEL Device acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the ZyXEL Device does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

Channel

A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference.

Wireless Mode

The IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. Your ZyXEL Device can support **802.11b Only**, **802.11g Only** and **802.11b+g**.

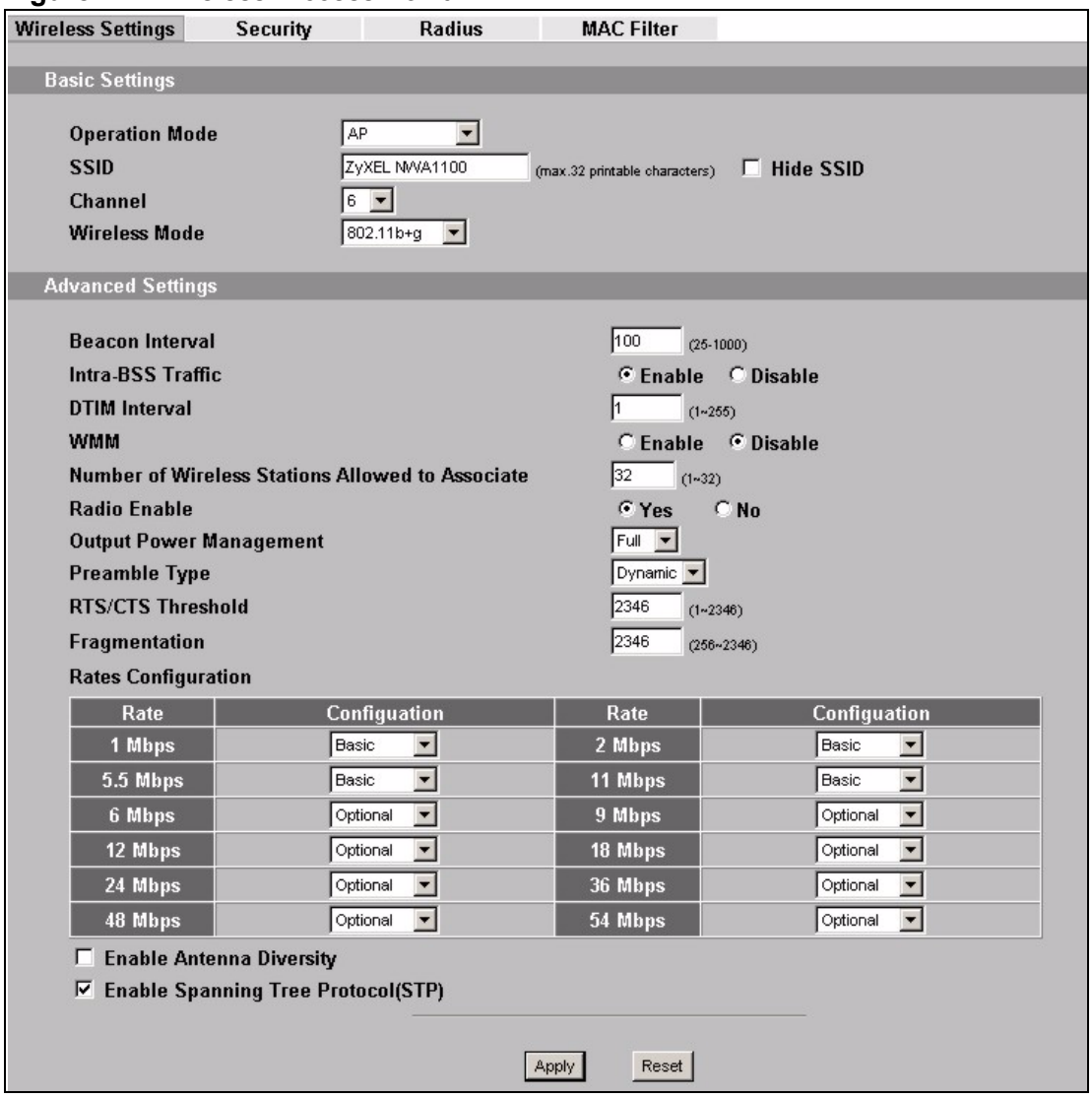
6.4 Wireless Settings Screen

Use this screen to choose the operating mode for your ZyXEL Device. Click **Wireless > Wireless Settings**. The screen varies depending upon the operating mode you select.

6.4.1 Access Point Mode

Use this screen to use your ZyXEL Device as an access point. Select **AP** as the **Operation Mode.** The following screen displays.

Figure 27 Wireless: Access Point



The following table describes the general wireless LAN labels in this screen.

Table 9 Wireless: Access Point

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select **AP** from the drop-down list.

Table 9 Wireless: Access Point

LABEL	DESCRIPTION
SSID	The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. Select an **SSID Profile** from the drop-down list box. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Hide SSID	If you hide the SSID, then the ZyXEL Device cannot be seen when a wireless client scans for local APs. The trade-off for the extra security of "hiding" the ZyXEL Device may be inconvenience for some valid WLAN clients.
Channel	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Wireless Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Advanced Settings	
Beacon Interval	When a wirelessly networked device sends a beacon, it includes with it a beacon interval. This specifies the time period before the device sends the beacon again. The interval tells receiving devices on the network how long they can wait in lowpower mode before waking up to handle the beacon. This value can be set from 20ms to 1000ms. A high value helps save current consumption of the access point.
Intra-BSS Traffic	When Intra-BSS is enabled, wireless client can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client can still access the wired network but cannot communicate with each other.

Table 9 Wireless: Access Point

LABEL	DESCRIPTION
DTIM Interval	Delivery Traffic Indication Message (DTIM) is the time period after which broadcast and multicast packets are transmitted to mobile clients in the Power Saving mode. A high DTIM value can cause clients to lose connectivity with the network. This value can be set from 1 to 100.
WMM	Select this to turn on WMM QoS (Wireless MultiMedia Quality of Service). The ZyXEL Device assigns priority to packets based on the IEEE 802.1q or DSCP information in their headers. If a packet has no WMM information in its header, it is assigned the default priority.
Number of Wireless Stations Allowed to Associate	Specify how many wireless stations can associate with your ZyXEL Device.
Radio Enable	Select **Yes** to enable WLAN radio, and **No** to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.
Output Power Management	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following **Full** (Full Power), **50%**, **25%**, **12.5%** or **Min** (Minimum). See the product specifications for more information on your ZyXEL Device's output power.
Preamble Type	Select Dynamic to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble. Select Long if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (1) turns on the RTS/CTS handshake. Enter a value between **1** and **2346**.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.

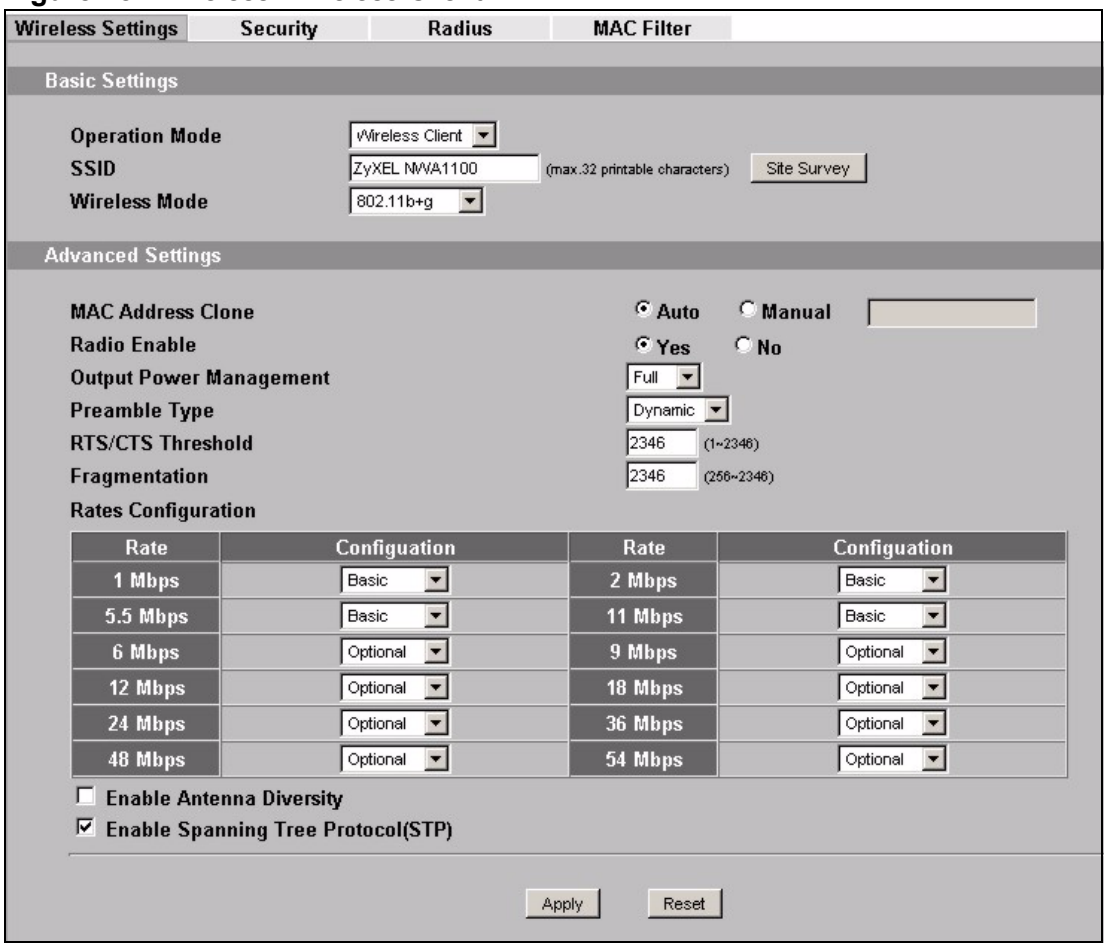
Table 9 Wireless: Access Point

LABEL	DESCRIPTION
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4.2 Wireless Client Mode

Use this screen to turn your ZyXEL Device into a wireless client. Select **Wireless Client** as the **Operation Mode**. The following screen displays.

Figure 28 Wireless: Wireless Client



The following table describes the general wireless LAN labels in this screen.

Table 10 Wireless: Wireless Client

LABEL	DESCRIPTION
Basic Settings	
Operation Mode	Select **Wireless Client** from the drop-down list. Click **Apply** to make the **Site Survey** button appear next to the **SSID** field. Click this button to get a pop up window of available APs.
SSID	The SSID (Service Set IDentifier) identifies the Service Set with which a wireless station is associated. Wireless stations associating to the access point (AP) must have the same SSID. In this field, enter the SSID of the AP you want to use (click **Site Survey** button for a list of available APs). Click **Apply**. Set the security configuration for this operating mode in the **Wireless > Security** screen. Check the **Status** screen to check if the settings you set show in the WLAN information. Note: If you are configuring the ZyXEL Device from a computer connected to the wireless LAN and you change the ZyXEL Device's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the ZyXEL Device's new settings.
Site Survey	Click this to view a list of available wireless access points within the range.
Wireless Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
Advanced Settings	
MAC Address Clone	Choose **Manual** to configure the ZyXEL Device's MAC address by cloning the MAC address from a computer on your LAN. Choose **Auto** to use the factory default MAC address of your ZyXEL Device.
Radio Enable	Select **Yes** to enable WLAN radio, and **No** to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.
Output Power Management	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following **Full** (Full Power), **50%**, **25%**, **12.5%** or **Min** (Minimum). See the product specifications for more information on your ZyXEL Device's output power.
Preamble Type	Select Dynamic to have the ZyXEL Device automatically use short preamble when the wireless network your ZyXEL Device is connected to supports it, otherwise the ZyXEL Device uses long preamble. Select Long preamble if you are unsure what preamble mode the wireless device your ZyXEL Device is connected to supports, and to provide more reliable communications in busy wireless networks.

Table 10 Wireless: Wireless Client

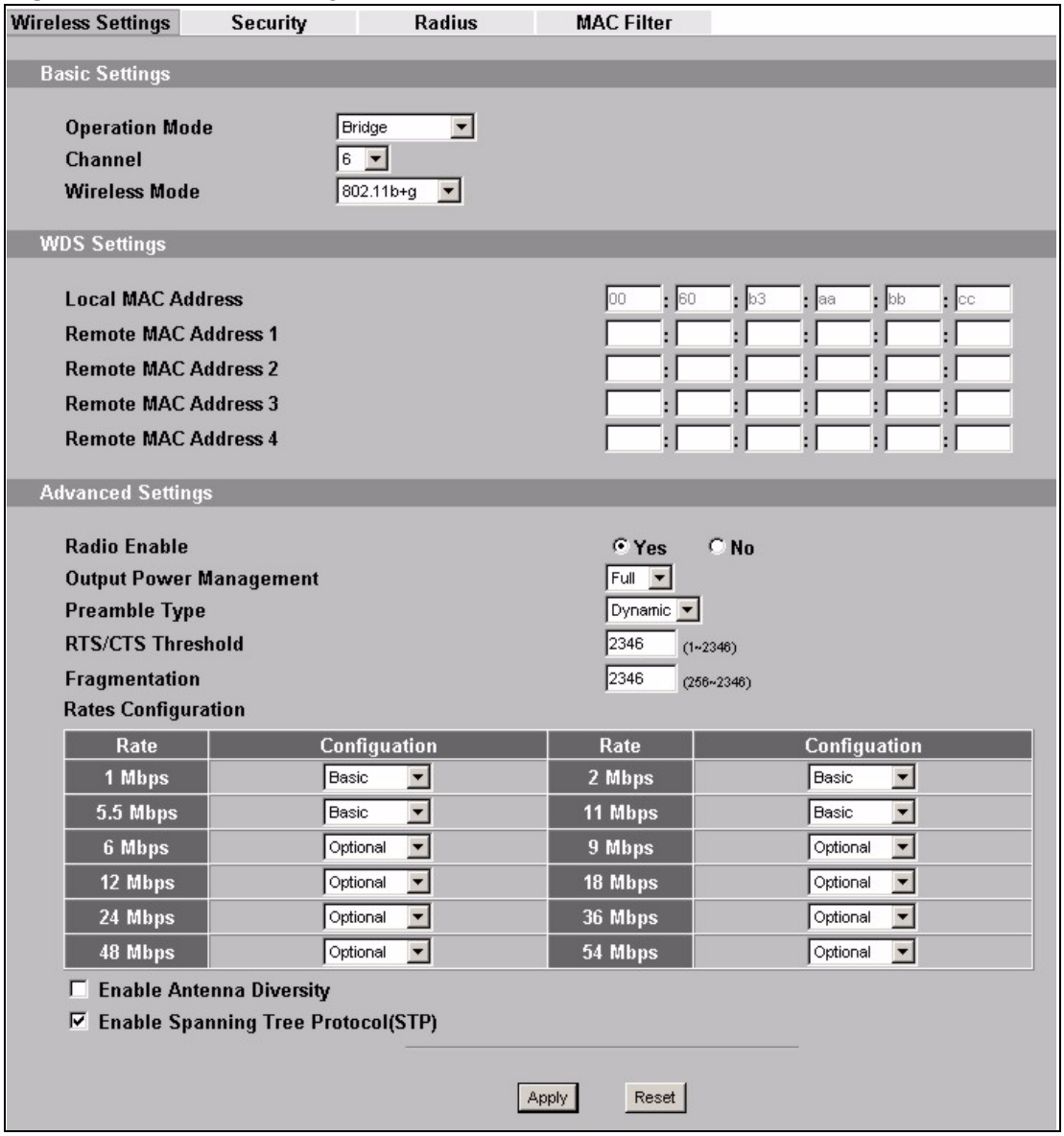
LABEL	DESCRIPTION
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to its smallest value (1) turns on the RTS/CTS handshake. Enter a value between **1** and **2346**.
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Spanning Tree Control (STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

6.4.3 Bridge Mode

Use this screen to have the ZyXEL Device act as a wireless network bridge and establish wireless links with other APs. You need to know the MAC address of the peer device, which also must be in bridge mode.

Use this screen to use the ZyXEL Device as a wireless bridge. Select **Bridge** as the **Operation Mode**.

Figure 29 Wireless: Bridge



The following table describes the bridge labels in this screen.

Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Basic Settings	
Operation Mode	Select **Bridge** in this field.

Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Channel	Set the operating frequency/channel depending on your particular region. To manually set the ZyXEL Device to use a channel, select a channel from the drop-down list box. Click **MAINTENANCE** and then the **Channel Usage** tab to open the **Channel Usage** screen to make sure the channel is not already used by another AP or independent peer-to-peer wireless network. To have the ZyXEL Device automatically select a channel, click **Scan** instead.
Wireless Mode	Select **802.11b Only** to allow only IEEE 802.11b compliant WLAN devices to associate with the ZyXEL Device. Select **802.11g Only** to allow only IEEE 802.11g compliant WLAN devices to associate with the ZyXEL Device. Select **802.11b+g** to allow both IEEE802.11b and IEEE802.11g compliant WLAN devices to associate with the ZyXEL Device. The transmission rate of your ZyXEL Device might be reduced.
WDS Settings	
Local Mac Address Remote MAC Address 1 - 4	A Wireless Distribution System is a wireless connection between two or more APs. Note: WDS security is independent of the security settings between the ZyXEL Device and any wireless clients. **Local MAC Address** is the MAC address of your ZyXEL Device. You can specify up to 4 remote devices' MAC addresses in this section.
Advanced Settings	
Radio Enable	Select **Yes** to enable WLAN radio, and **No** to turn it off. The ZyXEL Device cannot be accessed wirelessly if radio is turned off.
Output Power Management	Set the output power of the ZyXEL Device in this field. If there is a high density of APs in an area, decrease the output power of the ZyXEL Device to reduce interference with other APs. Select one of the following **Full** (Full Power), **50%**, **25%**, **12.5%** or **Min** (Minimum). See the product specifications for more information on your ZyXEL Device's output power.
Preamble Type	Select Dynamic to have the ZyXEL Device automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble. Select Long preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.
RTS/CTS Threshold	(Request To Send) The threshold (number of bytes) for enabling RTS/CTS handshake. Data with its frame size larger than this value will perform the RTS/CTS handshake. Setting this attribute to be larger than the maximum MSDU (MAC service data unit) size turns off the RTS/CTS handshake. Setting this attribute to 1 turns on the RTS/CTS handshake. Enter a value between **1** and **2346**.

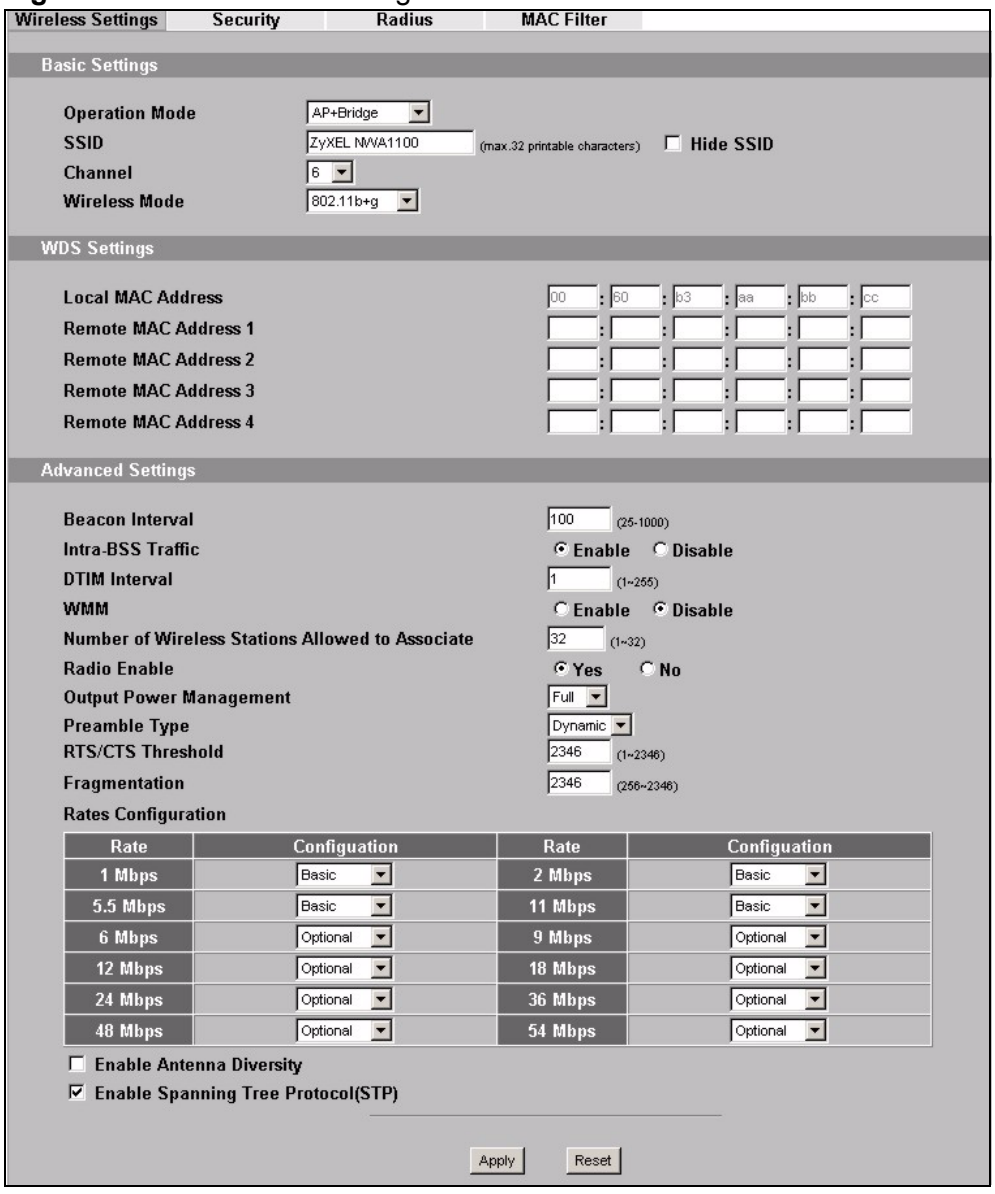
Table 11 Wireless: Bridge

LABEL	DESCRIPTIONS
Fragmentation	The threshold (number of bytes) for the fragmentation boundary for directed messages. It is the maximum data fragment size that can be sent. Enter an even number between **256** and **2346**.
Rates Configuration	This section controls the data rates permitted for clients. For each **Rate**, select an option from the **Configuration** list. The options are: • **Basic** (1~11 Mbps only): Clients can always connect to the access point at this speed. • **Optional**: Clients can connect to the access point at this speed, when permitted to do so by the AP. • **Disable**: Clients cannot connect to the access point at this speed.
Enable Antenna Diversity	Select this to use antenna diversity. Antenna diversity uses multiple antennas to reduce signal interference.
Enable Spanning Tree Protocol(STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP -compliant bridges in your network to ensure that only one path exists between any two stations on the network. Select the check box to activate STP on the ZyXEL Device.

6.4.4 AP + Bridge Mode

Use this screen to have the ZyXEL Device function as a bridge and access point simultaneously. Select **AP + Bridge** as the **Operation Mode**. The following screen diplays.

Figure 30 Wireless: AP+Bridge



See the tables describing the fields in the **Access Point** and **Bridge** operating modes for descriptions of the fields in this screen.

6.5 Technical Reference

This section provides technical background information about the topics covered in this chapter. Refer to Appendix E on page 157 for further readings on Wireless LAN.

6.5.1 WMM QoS

WMM (Wi-Fi MultiMedia) QoS (Quality of Service) ensures quality of service in wireless networks. It controls WLAN transmission priority on packets to be transmitted over the wireless network.

WMM QoS prioritizes wireless traffic according to the delivery requirements of the individual and applications. WMM QoS is a part of the IEEE 802.11e QoS enhancement to certified Wi-Fi wireless networks.

On APs without WMM QoS, all traffic streams are given the same access priority to the wireless network. If the introduction of another traffic stream creates a data transmission demand that exceeds the current network capacity, then the new traffic stream reduces the throughput of the other traffic streams.

The ZyXEL Device uses WMM QoS to prioritize traffic streams according to the IEEE 802.1q or DSCP information in each packet's header. The ZyXEL Device automatically determines the priority to use for an individual traffic stream. This prevents reductions in data transmission for applications that are sensitive to latency and jitter (variations in delay).

6.5.2 Spanning Tree Protocol (STP)

STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other STP-compliant bridges in your network to ensure that only one route exists between any two stations on the network.

6.5.2.1 Rapid STP

The ZyXEL Device uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allow faster convergence of the spanning tree (while also being backwards compatible with STP-only aware bridges). Using RSTP topology change information does not have to propagate to the root bridge and unwanted learned addresses are flushed from the filtering database. In RSTP, the port states are Discarding, Learning, and Forwarding.

6.5.2.2 STP Terminology

The root bridge is the base of the spanning tree; it is the bridge with the lowest identifier value (MAC address).

Path cost is the cost of transmitting a frame onto a LAN through that port. It is assigned according to the speed of the link to which a port is attached. The slower the media, the higher the cost - see the following table.

Table 12 STP Path Costs

	LINK SPEED	RECOMMENDED VALUE	RECOMMENDED RANGE	ALLOWED RANGE
Path Cost	4Mbps	250	100 to 1000	1 to 65535
Path Cost	10Mbps	100	50 to 600	1 to 65535
Path Cost	16Mbps	62	40 to 400	1 to 65535
Path Cost	100Mbps	19	10 to 60	1 to 65535
Path Cost	1Gbps	4	3 to 10	1 to 65535
Path Cost	10Gbps	2	1 to 5	1 to 65535

On each bridge, the root port is the port through which this bridge communicates with the root. It is the port on this switch with the lowest path cost to the root (the root path cost). If there is no root port, then this bridge has been accepted as the root bridge of the spanning tree network.

For each LAN segment, a designated bridge is selected. This bridge has the lowest cost to the root among the bridges connected to the LAN.

6.5.2.3 How STP Works

After a bridge determines the lowest cost-spanning tree with STP, it enables the root port and the ports that are the designated ports for connected LANs, and disables all other ports that participate in STP. Network packets are therefore only forwarded between enabled ports, eliminating any possible network loops.

STP-aware bridges exchange Bridge Protocol Data Units (BPDUs) periodically. When the bridged LAN topology changes, a new spanning tree is constructed.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a Hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology.

6.5.2.4 STP Port States

STP assigns five port states (see next table) to eliminate packet looping. A bridge port is not allowed to go directly from blocking state to forwarding state so as to eliminate transient loops.

Table 13 STP Port States

PORT STATES	DESCRIPTIONS
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

6.5.3 Additional Wireless Terms

Table 14 Additional Wireless Terms

TERM	DESCRIPTION
Intra-BSS Traffic	This describes direct communication (not through the ZyXEL Device) between two wireless devices within a wireless network. You might disable this kind of communication to enhance security within your wireless network.
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the ZyXEL Device. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the ZyXEL Device.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the ZyXEL Device does, it cannot communicate with the ZyXEL Device.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

TERM	DESCRIPTION
Roaming	If you have two or more ZyXEL Devices (or other wireless access points) on your wireless network, you can enable this option so that wireless devices can change locations without having to log in again. This is useful for devices, such as notebooks, that move around a lot.
Antenna	An antenna couples Radio Frequency (RF) signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air. Positioning the antennas properly increases the range and coverage area of a wireless LAN.

7

Wireless Security Screen

7.1 Overview

This chapter describes how to use the **Wireless Security** screen. This screen allows you to configure the security mode for your ZyXEL Device.

Wireless security is vital to your network. It protects communications between wireless stations, access points and the wired network.

Figure 31 Securing the Wireless Network

In the figure above, the ZyXEL Device checks the identity of devices before giving them access to the network. In this scenario, Computer A is denied access to the network, while Computer B is granted connectivity.

The ZyXEL Device secure communications via data encryption, wireless client authentication and MAC address filtering. It can also hide its identity in the network.

7.2 What You Can Do in the Wireless Security Screen

Use the **Wireless > Security** screen (see Section 7.4 on page 76) to choose the security mode for your ZyXEL Device.

7.3 What You Need To Know About Wireless Security

User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

The following table shows the relative effectiveness of wireless security methods:.

Table 15 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

The available security modes in your ZyXEL Device are as follows:

- **None.** No data encryption.
- **WEP.** Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between the wireless stations and the access points to keep network communications private.
- **802.1x-Only.** This is a standard that extends the features of IEEE 802.11 to support extended authentication. It provides additional accounting and control features. This option does not support data encryption.

- **802.1x-Static64.** This provides 802.1x-Only authentication with a static 64bit WEP key and an authentication server.
- **802.1x-Static128**. This provides 802.1x-Only authentication with a static 128bit WEP key and an authentication server.
- **WPA.** Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard.
- **WPA2.** WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.
- **WPA2-MIX.** This commands the ZyXEL Device to use either WPA2 or WPA depending on which security mode the wireless client uses.
- **WPA2-PSK**. This adds a pre-shared key on top of WPA2 standard.
- **WPA2-PSK-MIX**. This commands the ZyXEL Device to use either WPA-PSK or WPA2-PSK depending on which security mode the wireless client uses.

Note: In **Bridge** and **Bridge + AP** operating modes, the only available security modes are **WEP** and **WPA2-PSK**.

Passphrase

A passphrase functions like a password. In WEP security mode, it is further converted by the ZyXEL Device into a complicated string that is referred to as the "key". This key is requested from all devices wishing to connect to a wireless network.

PSK

The Pre-Shared Key (PSK) is a password shared by a wireless access point and a client during a previous secure connection. The key can then be used to establish a connection between the two parties.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message. Encryption is the process of converting data into unreadable text. This secures information in network communications. The intended recipient of the data can "unlock" it with a pre-assigned key, making the information readable only to him. The ZyXEL Device when used as a wireless client employs Temporal Key Integrity Protocol (TKIP) data encryption.

EAP

Extensible Authentication Protocol (EAP) is a protocol used by a wireless client, an access point and an authentication server to negotiate a connection.

The EAP methods employed by the ZyXEL Device when in Wireless Client operating mode are Transport Layer Security (TLS), Protected Extensible

Authentication Protocol (PEAP), Lightweight Extensible Authentication Protocol (LEAP) and Tunneled Transport Layer Security (TTLS). The authentication protocol may either be Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) or Generic Token Card (GTC).

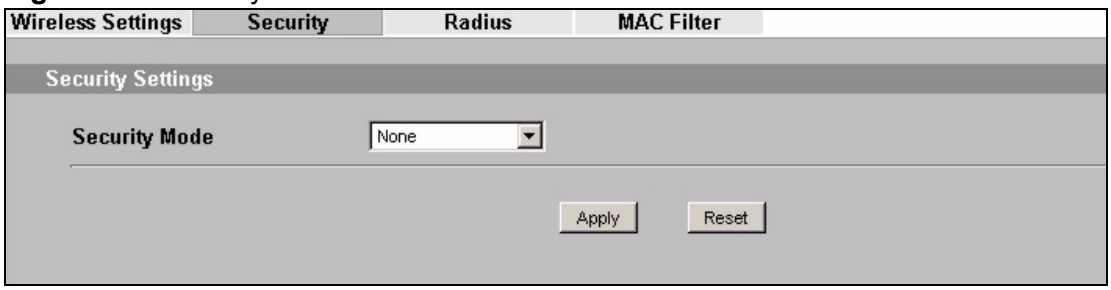
Further information on these terms can be found in Appendix E on page 157.

7.4 The Security Screen

Use this screen to choose the security mode for your ZyXEL Device.

Click **Wireless > Security**. The screen varies depending upon the security mode you select.

Figure 32 Security: None



The default security mode is set to **None**.

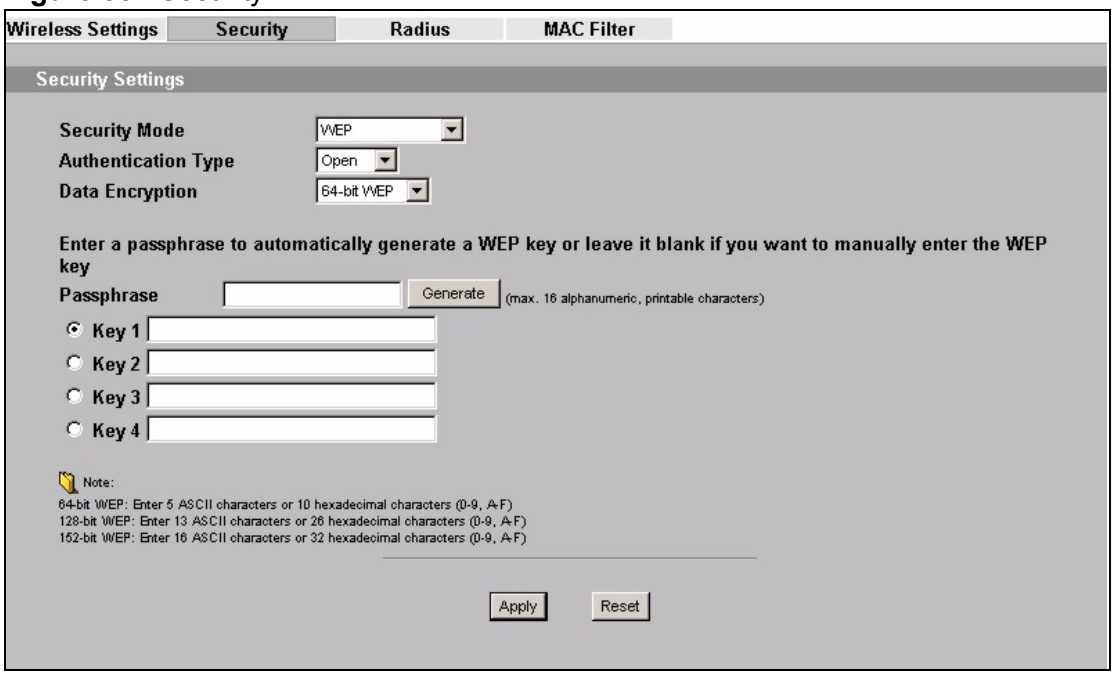
Note that some screens display differently depending on the operating mode selected in the **Wireless > Wireless Settings** screen.

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

7.4.1 Security: WEP

Use this screen to use WEP as the security mode for your ZyXEL Device. Select **WEP** in the **Security Mode** field to display the following screen.

Figure 33 Security: WEP



The following table describes the labels in this screen.

Table 16 Security: WEP

LABEL	DESCRIPTION
Security Mode	Choose **WEP** in this field.
Authentication Method	Select **Open** or **Shared Key** from the drop-down list box. The default setting is **Auto**.
Data Encryption	Select **Disable** to allow wireless stations to communicate with the access points without any data encryption. Select **64-bit WEP**, **128-bit WEP** or **152-bit WEP** to enable data encryption.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters.
Generate	Click this to get the keys from the **Passphrase** you entered.

Table 16 Security: WEP

LABEL	DESCRIPTION
Key 1 to Key 4	The WEP keys are used to encrypt data. Both the ZyXEL Device and the wireless stations must use the same WEP key for data transmission. If you chose **64-bit WEP**, then enter any 5 ASCII characters or 10 hexadecimal characters ("0-9", "A-F"). If you chose **128-bit WEP**, then enter 13 ASCII characters or 26 hexadecimal characters ("0-9", "A-F"). If you chose **152-bit WEP**, then enter 16 ASCII characters or 32 hexadecimal characters ("0-9", "A-F"). You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

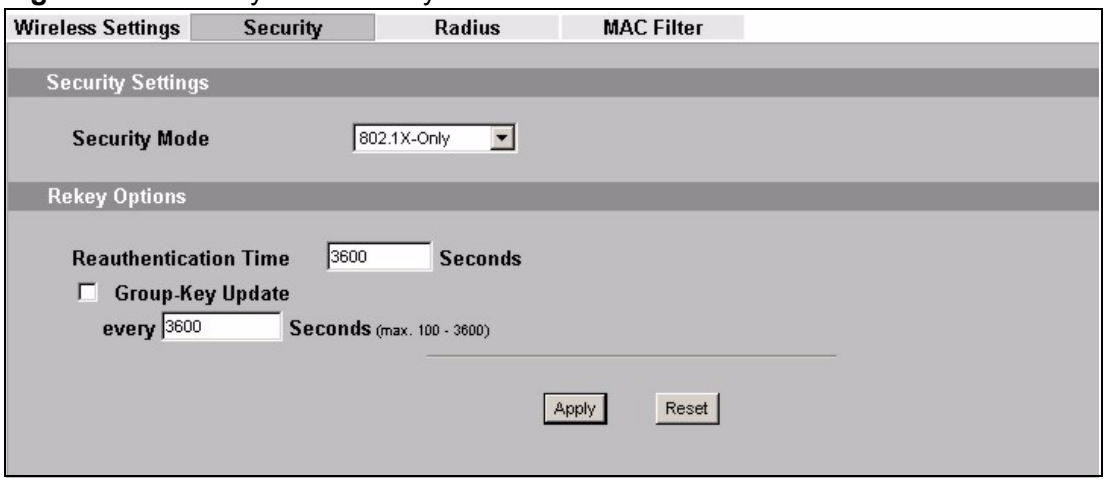
7.4.2 Security: 802.1x Only

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.2.1 Access Point

Use this screen to use 802.1x-Only security mode for your ZyXEL Device that is in Access Point operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 34 Security: 802.1x Only for Access Point



The following table describes the labels in this screen.

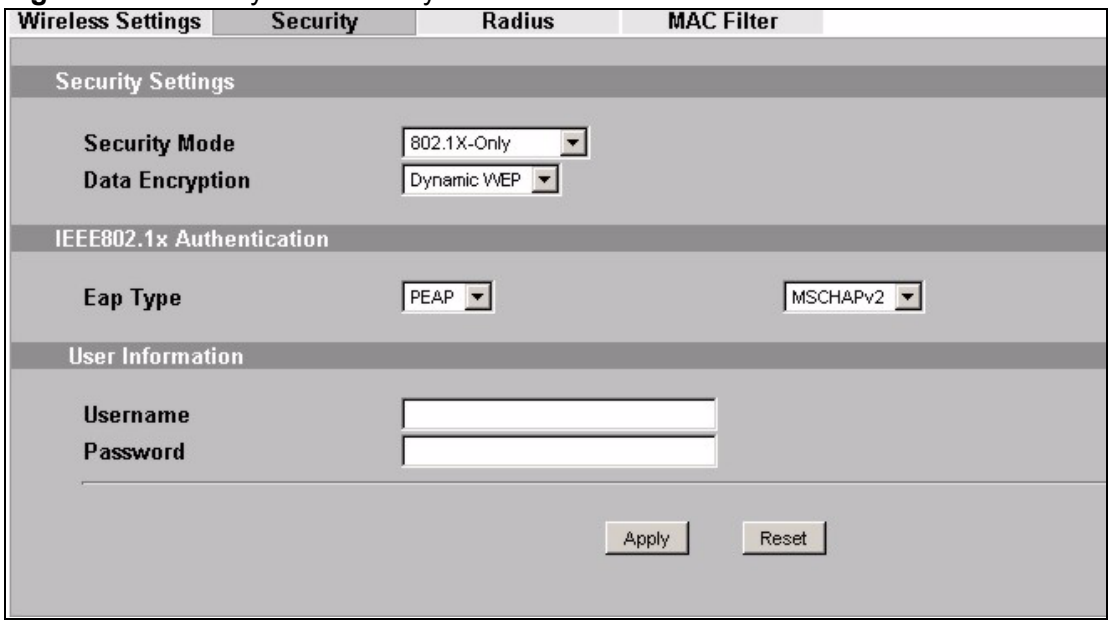
Table 17 Security: 802.1x Only for Access Point

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose **802.1x Only** in this field.
Rekey Options	
ReAuthentication Time	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group-Key Update	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.2.2 Wireless Client

Use this screen to use 802.1x-Only security mode for your ZyXEL Device that is in Wireless Client operating mode. Select **802.1x-Only** in the **Security Mode** field to display the following screen.

Figure 35 Security: 802.1x Only for Wireless Client



The following table describes the labels in this screen.

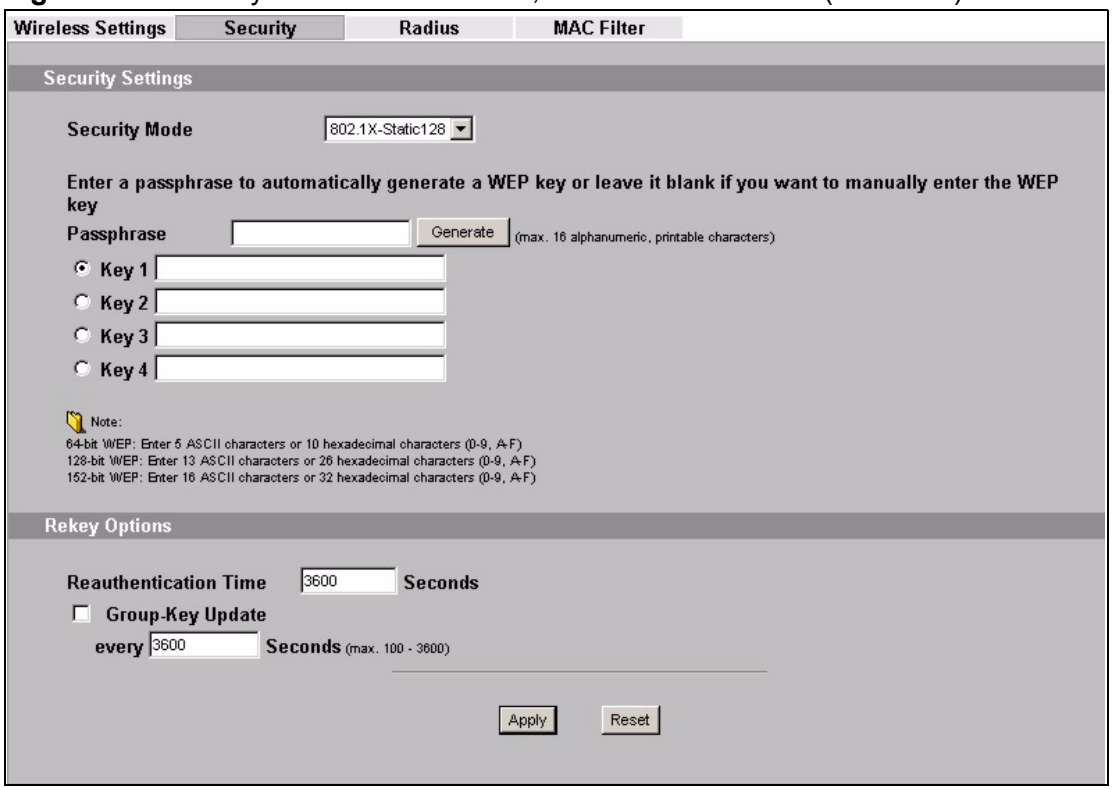
Table 18 Security: 802.1x Only for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **Dynamic WEP**. Refer to Section on page 166 for information on using Dynamic WEP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.3 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

Use this screen to use 802.1x Static 64 or 802.1x Static 128 security mode for your ZyXEL Device. Select **802.1x Static 64** or **802.1x Static 128** in the **Security Mode** field to display the following screen.

Figure 36 Security: 802.1x Static 64-bit, 802.1x Static 128-bit (AP mode)



The following table describes the labels in this screen.

Table 19 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose **802.1x Static 64 or 802.1x Static 128** in this field.
Passphrase	Enter the passphrase or string of text used for automatic WEP key generation on wireless client adapters (AP mode).
Generate	Click this to get the keys from the **Passphrase** you entered (AP mode).

Table 19 Security: 802.1x Static 64-bit, 802.1x Static 128-bit

LABEL	DESCRIPTION
Key 1 to Key 4	If you chose **802.1x Static 64**, then enter any 5 characters (ASCII string) or 10 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. If you chose **802.1x Static 128-bit**, then enter 13 characters (ASCII string) or 26 hexadecimal characters ("0-9", "A-F") preceded by 0x for each key. There are four data encryption keys to secure your data from eavesdropping by unauthorized wireless users. The values for the keys must be set up exactly the same on the access points as they are on the wireless stations. The preceding "0x" is entered automatically. You must configure all four keys, but only one key can be activated at any one time. The default key is key 1.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group-Key Update	The ZyXEL Device automatically disconnects a wireless station from the wired network after a period of inactivity. The wireless station needs to enter the user name and password again before access to the wired network is allowed. The default time interval is **3600** seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

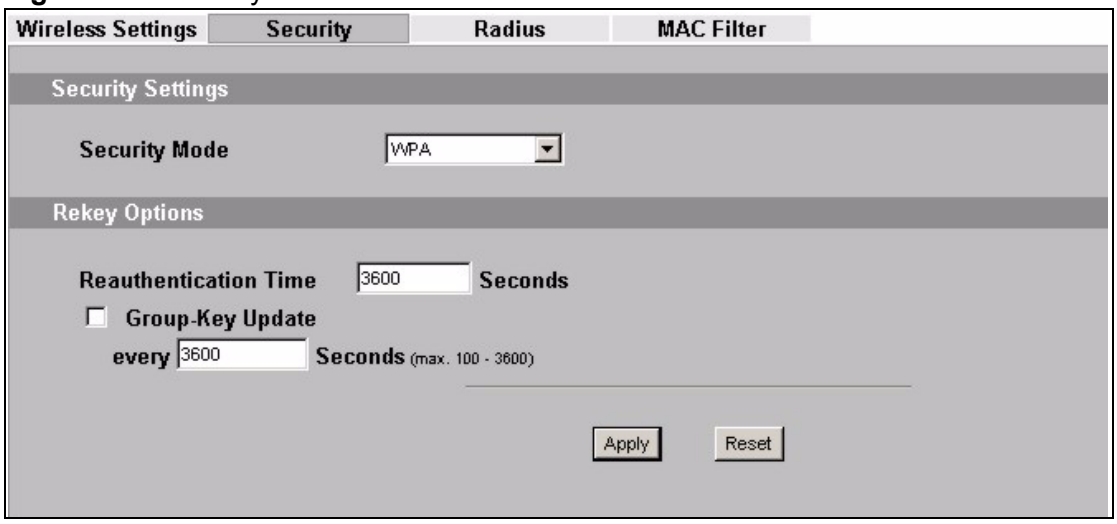
7.4.4 Security: WPA

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.4.1 Access Point

Use this screen to employ WPA as the security mode for your ZyXEL Device that is in Access Point operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 37 Security: WPA for Access Point



The following table describes the labels in this screen.

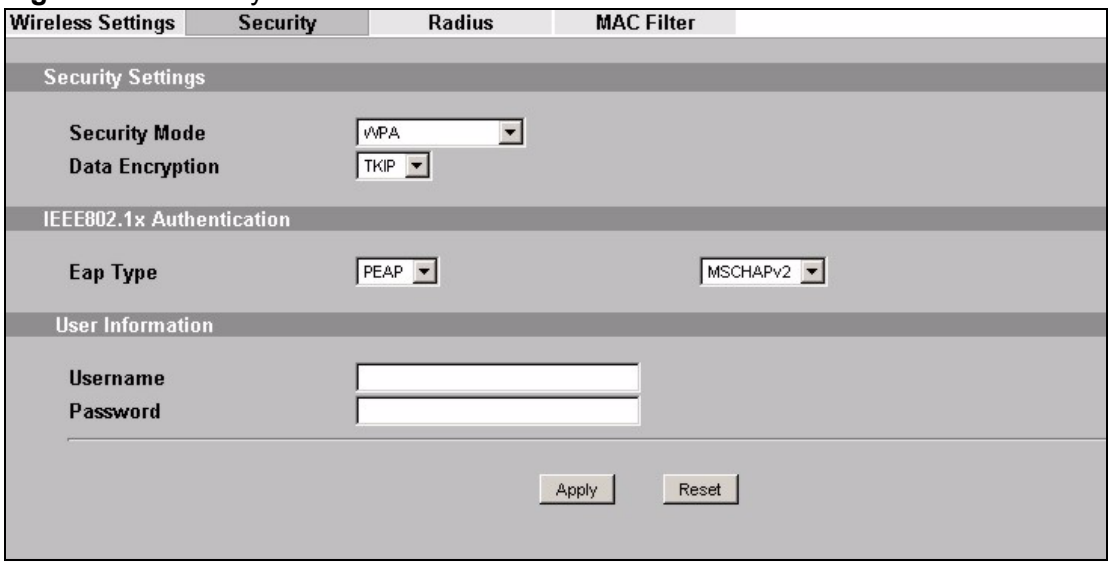
Table 20 Security: WPA for Access Point

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose **WPA** in this field.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend user names and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device default is 3800 seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.4.2 Wireless Client

Use this screen to employ WPA as the security mode for your ZyXEL Device that is in Wireless Client operating mode. Select **WPA** in the **Security Mode** field to display the following screen.

Figure 38 Security: WPA for Wireless Client



The following table describes the labels in this screen.

Table 21 Security: WPA for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose the same security mode used by the AP.
Data Encryption	Select between **None** and **TKIP**.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

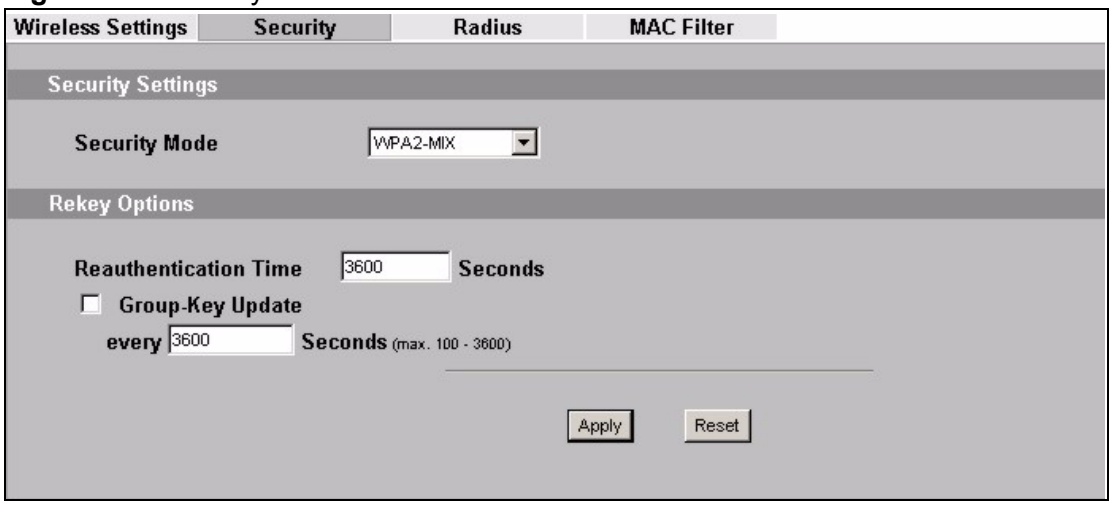
7.4.5 Security: WPA2 or WPA2-MIX

This screen varies depending on whether you select **Access Point** or **Wireless Client** in the **Wireless > Wireless Settings** screen.

7.4.5.1 Access Point

Use this screen to use WAP2 or WPA2-MIX as the security mode for your ZyXEL Device that is in Access Point operating mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 39 Security:WPA2 or WPA2-MIX for Access Point



The following table describes the labels not previously discussed

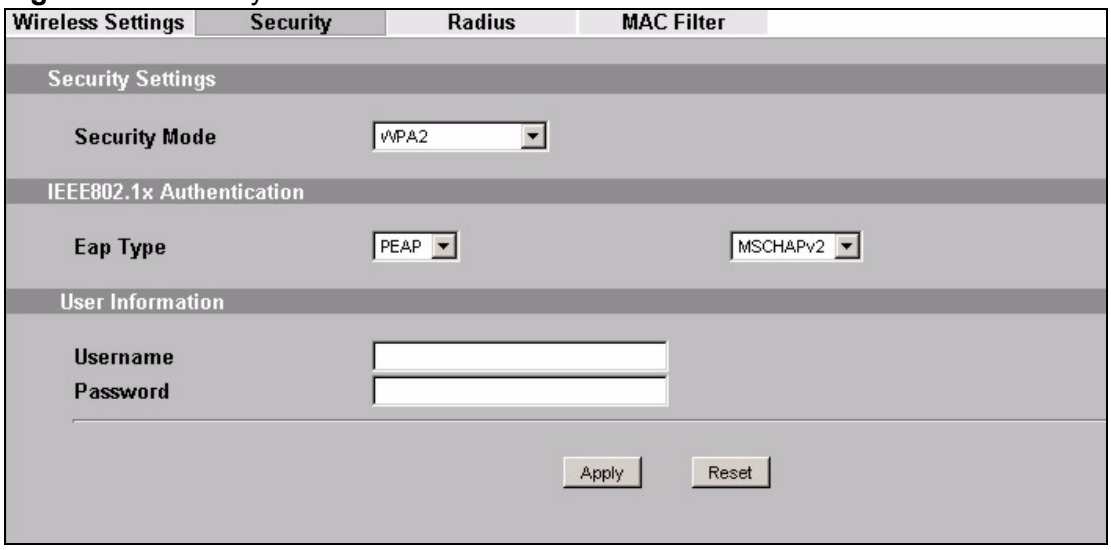
Table 22 Security: WPA2 or WPA2-MIX for Access Point

LABEL	DESCRIPTIONS
Security Settings	
Security Mode	Choose **WPA2** or **WPA2-MIX** in this field.
Rekey Options	
ReAuthentication Timer	Specify how often wireless stations have to resend usernames and passwords in order to stay connected. Enter a time interval between 10 and 9999 seconds. The default time interval is **1800** seconds (30 minutes). Alternatively, enter "0" to turn reauthentication off. Note: If wireless station authentication is done using a RADIUS server, the reauthentication timer on the RADIUS server has priority.
Group Key Update Timer	The **Group Key Update Timer** is the rate at which the AP sends a new group key out to all clients. The re-keying process is the WPA equivalent of automatically changing the group key for an AP and all stations in a WLAN on a periodic basis. Setting of the **Group Key Update Timer** is also supported in WPA-PSK mode. The ZyXEL Device's default is 3600 seconds (or 1 hour).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.5.2 Wireless Client

Use this screen to employ WPA2 or WPA2-MIX as the security mode of your ZyXEL Device that is in Wireless Client operating mode. Select **WPA2** or **WPA2-MIX** in the **Security Mode** field to display the following screen.

Figure 40 Security: WPA2 or WPA2-MIX for Wireless Client



The following table describes the labels in this screen.

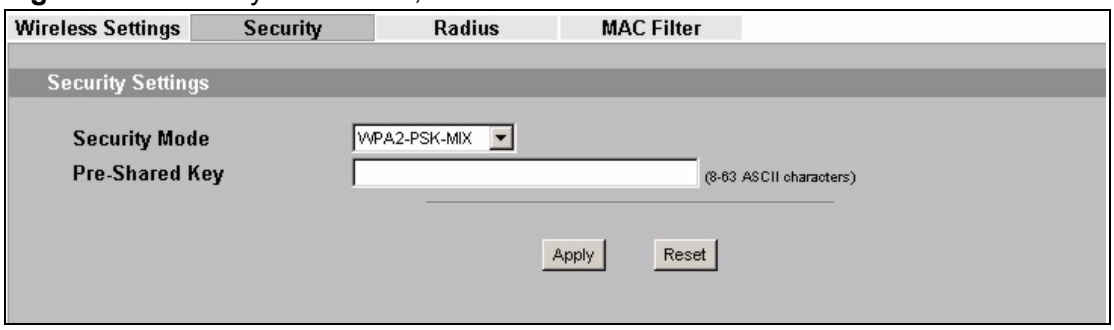
Table 23 Security: WPA2 or WPA2-MIX for Wireless Client

LABEL	DESCRIPTION
Security Settings	
Security Mode	Choose the same security mode used by the AP.
IEEE802.1x Authentication	
EAP Type	The options on the left refer to EAP methods. You can choose either **TLS, LEAP, PEAP** or **TTLS.** The default value is PEAP. The options on the right refer to authentication protocols. You can choose between **MSCHAPv2** and **GTC**.The default value is MSCHAPv2.
User Information	
Username	Supply the username of the account created in the RADIUS server.
Password	Supply the password of the account created in the RADIUS server.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.4.6 Security: WPA-PSK, WPA2-PSK, WPA2-PSK-MIX

Use this screen to employ WPA-PSK, WPA2-PSK or WPA2-PSK-MIX as the security mode of your ZyXEL Device. Select **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in the **Security Mode** field to display the following screen.

Figure 41 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX



The following table describes the labels not previously discussed

Table 24 Security: WPA-PSK, WPA2-PSK or WPA2-PSK-MIX

LABEL	DESCRIPTION
Security Mode	Choose **WPA-PSK**, **WPA2-PSK** or **WPA2-PSK-MIX** in this field.
Pre-Shared Key	The encryption mechanisms used for **WPA** and **WPA-PSK** are the same. The only difference between the two is that **WPA-PSK** uses a simple common password, instead of user-specific credentials. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

7.5 Technical Reference

This section provides technical background information on the topics discussed in this chapter.

The following is a general guideline in choosing the security mode for your ZyXEL Device.

- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.Use WPA(2) security if you have WPA(2)-aware wireless clients and a RADIUS server. WPA has user authentication and improved data encryption over WEP.
- Use WPA(2)-PSK if you have WPA(2)-aware wireless clients but no RADIUS server.

- If you don’t have WPA(2)-aware wireless clients, then use WEP key encrypting. A higher bit key offers better security. You can manually enter 64-bit, 128-bit or 152-bit WEP keys.

More information on Wireless Security can be found in Appendix E on page 157.

8

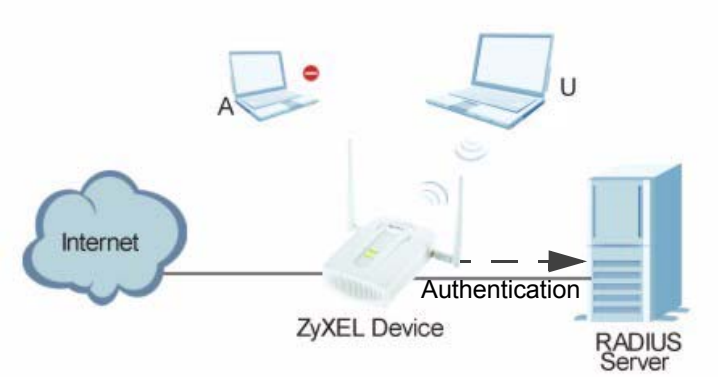
RADIUS Screen

8.1 Overview

This chapter describes how you can use the **Wireless > RADIUS** screen.

Remote Authentication Dial In User Service (RADIUS) is a protocol that can be used to manage user access to large networks. It is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server.

Figure 42 RADIUS Server Setup



In the figure above, wireless clients A and B are trying to access the Internet via the ZyXEL Device. The ZyXEL Device in turn queries the RADIUS server if the identity of clients A and U are allowed access to the Internet. In this scenario, only client U's identity is verified by the RADIUS server and allowed access to the Internet.

8.2 What You Can Do in the RADIUS Screen

Use the **Security > RADIUS** screen (see Section 7.4.1 on page 77) if you want to authenticate wireless users using a RADIUS Server and/or Accounting Server.

8.3 What You Need to Know About RADIUS

The RADIUS server handles the following tasks:

- **Authentication** which determines the identity of the users.
- **Authorization** which determines the network services available to authenticated users once they are connected to the network.
- **Accounting** which keeps track of the client's network activity.

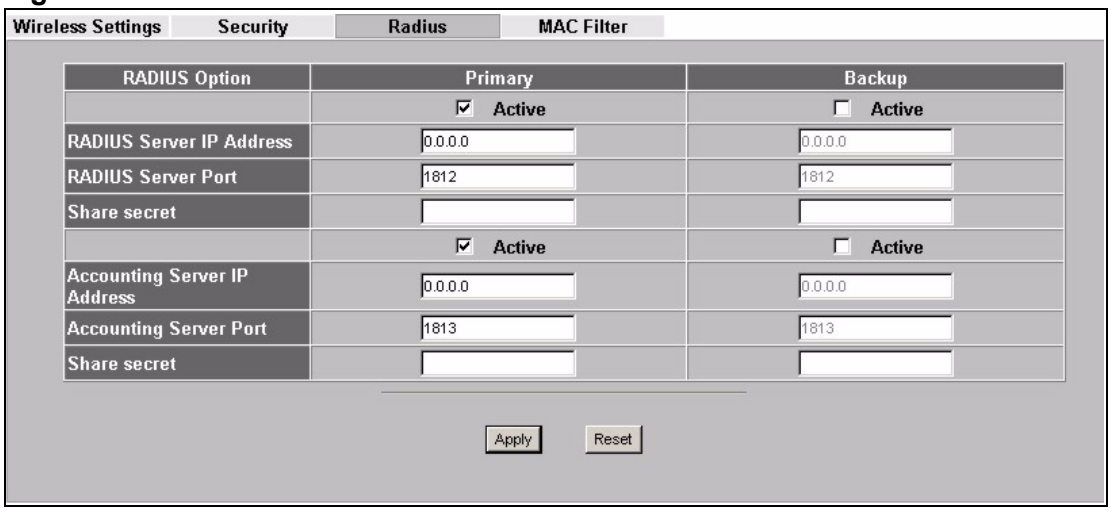
RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

You should know the IP addresses, ports and share secrets of the external RADIUS server and/or the external RADIUS accounting server you want to use with your ZyXEL Device. You can configure a primary and backup RADIUS and RADIUS accounting server for your ZyXEL Device.

8.4 The RADIUS Screen

Use this screen to set up your ZyXEL Device's RADIUS server settings. Click **Wireless** > **RADIUS**. The screen appears as shown.

Figure 43 Wireless > RADIUS



The following table describes the labels in this screen.

Table 25 Wireless > RADIUS

LABEL	DESCRIPTION
Primary	Configure the fields below to set up user authentication and accounting.
Backup	If the ZyXEL Device cannot communicate with the **Primary** accounting server, you can have the ZyXEL Device use a **Backup** RADIUS server. Make sure the **Active** check boxes are selected if you want to use backup servers. The ZyXEL Device will attempt to communicate three times before using the **Backup** servers. Requests can be issued from the client interface to use the backup server. The length of time for each authentication is decided by the wireless client or based on the configuration of the **ReAuthentication Timer** field in the **Security Settings** screen.
RADIUS Option	
Active	Select the check box to enable user authentication through an external authentication server. This check box is not available when you select **Internal**.
RADIUS Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation. This field is not available when you select **Internal**.
RADIUS Server Port	Enter the port number of the external authentication server. The default port number is 1812. You need not change this value unless your network administrator instructs you to do so. This field is not available when you select **Internal**.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external authentication server and the ZyXEL Device. The key must be the same on the external authentication server and your ZyXEL Device. The key is not sent over the network. This field is not available when you select **Internal**.
Active	Select the check box to enable user accounting through an external authentication server.
Accounting Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Accounting Server Port	Enter the port number of the external accounting server. The default port number is 1813. You need not change this value unless your network administrator instructs you to do so with additional information.
Share Secret	Enter a password (up to 128 alphanumeric characters) as the key to be shared between the external accounting server and the ZyXEL Device. The key must be the same on the external accounting server and your ZyXEL Device. The key is not sent over the network.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

9

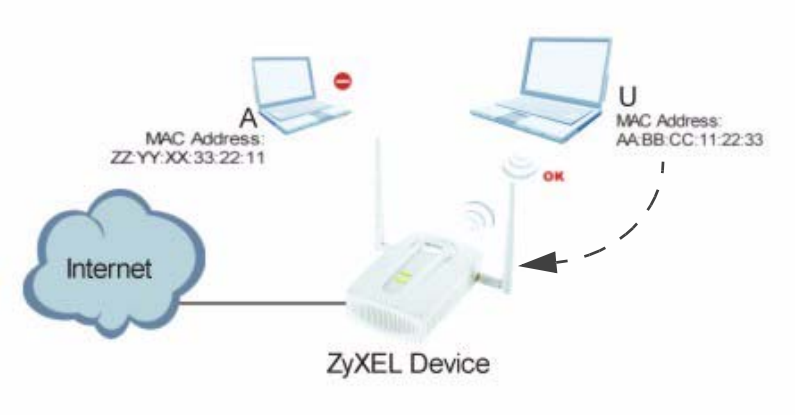
MAC Filter Screen

9.1 Overview

This chapter discusses how you can use the **Wireless > MAC Filter** screen.

The MAC filter function allows you to configure the ZyXEL Device to grant access to the ZyxEL Device from other wireless devices (Allow Association) or exclude devices from accessing the ZyXEL Device (Deny Association).

Figure 44 MAC Filtering



In the figure above, wireless client U is able to connect to the Internet because its MAC address is in the allowed association list specified in the ZyXEL Device. The MAC address of client A is either denied association or is not in the list of allowed wireless clients specified in the ZyXEL Device.

9.2 What You Can Do in the MAC Filter

Use the **Wireless > MAC Filter** screen (see Section 9.4 on page 94) to specify which wireless station is allowed or denied access to the ZyXEL Device.

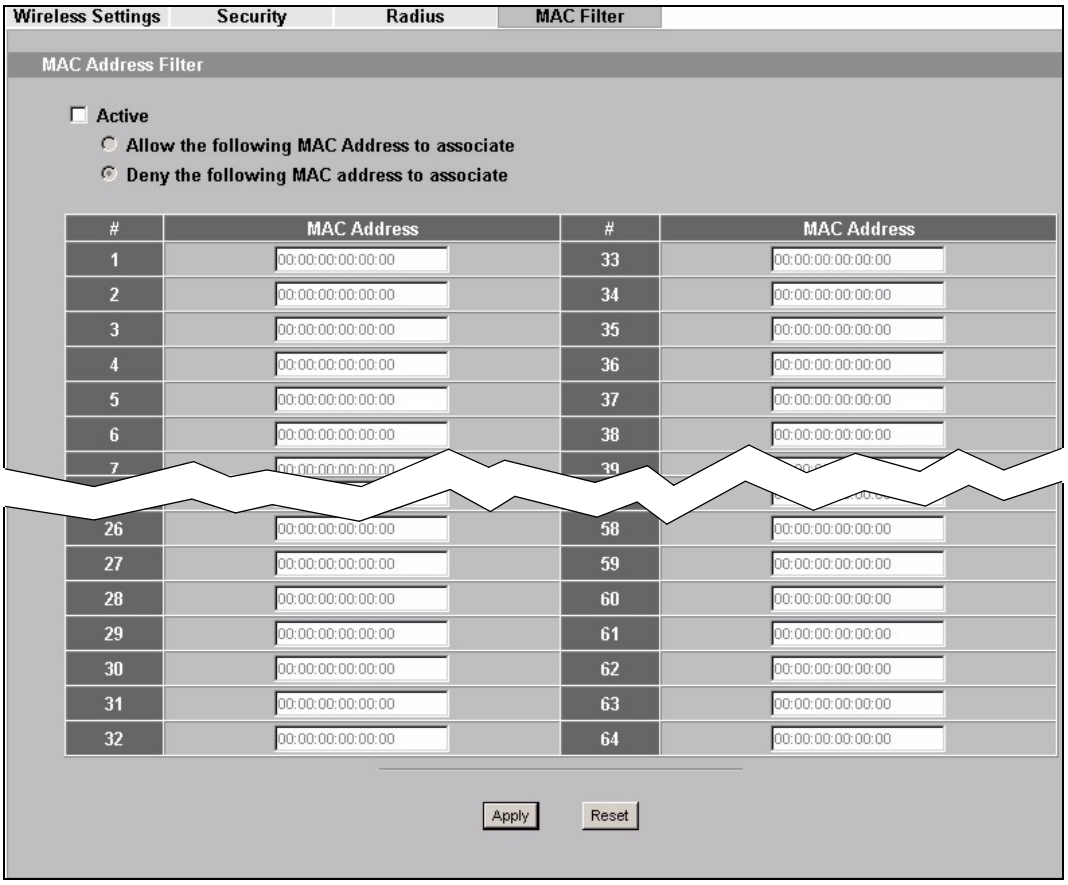
9.3 What You Need To Know About MAC Filter

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of each device to configure MAC filtering on the ZyXEL Device.

9.4 MAC Filter Screen

Use this screen to enable MAC address filtering in your ZyXEL Device.You can specify up to 64 MAC addresses to either allow or deny association with your ZyXEL Device. Click **Wireless > MAC Filter**. The screen displays as shown.

Figure 45 Wireless > MAC Filter



The following table describes the labels in this screen.

Table 26 Wireless > MAC Filter

LABEL	DESCRIPTION
Active	Click this to enable this feature.
Allow the following MAC Address to associate	Define the filter action for the list of MAC addresses in the MAC address filter table. Select this to permit access to the ZyXEL Device. MAC addresses not listed will be denied access to the ZyXEL Device.
Deny the following MAC Address to associate	Select this to block access to theZyXEL Device. MAC addresses not listed will be allowed to access the ZyXEL Device.
MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station to be allowed or denied access to the ZyXEL Device.
Description	Type a name to identify this wireless station.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10

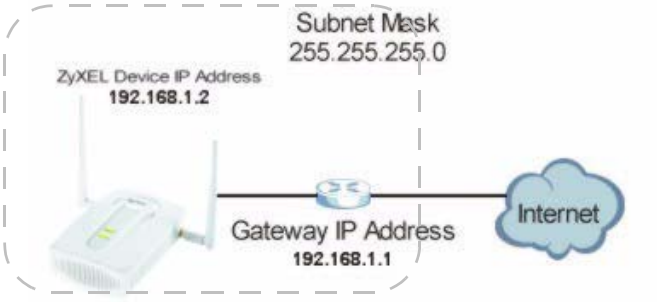
IP Screen

10.1 Overview

This chapter describes how you can configure the IP address of your ZyXEL Device.

The Internet Protocol (IP) address identifies a device on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Figure 46 IP Setup



The figure above illustrates one possible setup of your ZyXEL Device. The gateway IP address is 192.168.1.2 and the IP address of the ZyXEL Device is 192.168.1.2 (default). The gateway and the device must belong in the same subnet mask to be able to communicate with each other.

10.2 What You Can Do in the IP Screen

Use the **IP** screen (see Section 10.4 on page 98) to configure the IP address of your ZyXEL Device.

10.3 What You Need to Know About IP

The Ethernet parameters of the ZyXEL Device are preset in the factory with the following values:

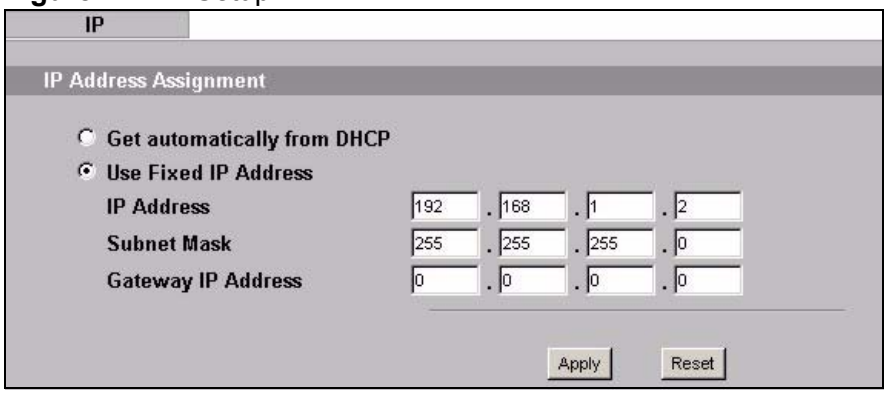
1 IP address of 192.168.1.2

2 Subnet mask of 255.255.255.0 (24 bits)

10.4 IP Screen

Use this screen to configure the IP address for your ZyXEL Device. Click **IP** to display the following screen.

Figure 47 IP Setup



The following table describes the labels in this screen.

Table 27 IP Setup

LABEL	DESCRIPTION
Get automatically from DHCP	Select this option if your ZyXEL Device is using a dynamically assigned IP address from a DHCP server each time. Note: You must know the IP address assigned to the ZyXEL Device (by the DHCP server) to access the ZyXEL Device again.
Use fixed IP address	Select this option if your ZyXEL Device is using a static IP address. When you select this option, fill in the fields below.
IP Address	Enter the IP address of your ZyXEL Device in dotted decimal notation. Note: If you change the ZyXEL Device's IP address, you must use the new IP address if you want to access the web configurator again.

Table 27 IP Setup

LABEL	DESCRIPTION
Subnet Mask	Type the subnet mask.
Gateway IP Address	Type the IP address of the gateway. The gateway is an immediate neighbor of your ZyXEL Device that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your ZyXEL Device; over the WAN, the gateway must be the IP address of one of the remote nodes.
Apply	Click **Apply** to save your changes.
Reset	Click **Reset** to begin configuring this screen afresh.

10.5 Technical Reference

This section provides the technical background information about the topics covered in this chapter.

10.5.1 WAN IP Address Assignment

Every computer on the Internet must have a unique IP address. If your networks are isolated from the Internet (only between your two branch offices, for instance) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks.

Table 28 Private IP Address Ranges

10.0.0.0	-	10.255.255.255
172.16.0.0	-	172.31.255.255
192.168.0.0	-	192.168.255.255

You can obtain your IP address from the IANA, from an ISP or have it assigned by a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

11

Remote Management

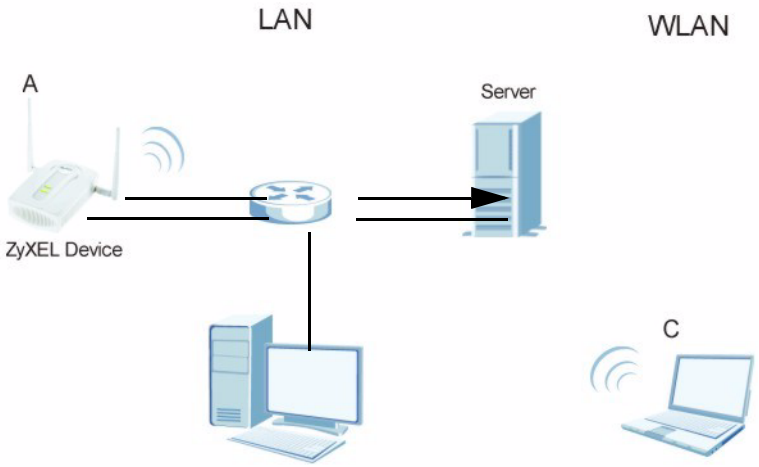
11.1 Overview

This chapter shows you how to enable remote management of your ZyXEL Device. It provides information on determining which services or protocols can access which of the ZyXEL Device's interfaces.

Remote Management allows a user to administrate the device over the network. You can manage your ZyXEL Device from a remote location via the following interfaces:

- WLAN
- LAN
- Both WLAN and LAN
- Neither (Disable)

Figure 48 Remote Management Example



In the figure above, the ZyXEL Device (A) is being managed by a desktop computer (B) connected via LAN (Land Area Network). It is also being accessed by a notebook (C) connected via WLAN (Wireless LAN).

11.2 What You Can Do in the Remote Management Screens

- Use the **Telnet** screen (see Section 11.4 on page 104) to configure through which interface(s) and from which IP address(es) you can use Telnet to manage the ZyXEL Device. A Telnet connection is prioritized by the ZyXEL Device over other remote management sessions.
- Use the **FTP** screen (see Section 11.5 on page 105) to configure through which interface(s) and from which IP address(es) you can use File Transfer Protocol (FTP) to manage the ZyXEL Device. You can use FTP to upload the latest firmware for example.
- Use the **WWW** screen (see Section 11.6 on page 106) to configure through which interface(s) and from which IP address(es) you can use the Web Browser to manage the ZyXEL Device.
- Use the **SNMP** screen (see Section 11.7 on page 107) to configure through which interface(s) and from which IP address(es) a network systems manager can access the ZyXEL Device.

11.3 What You Need To Know About Remote Management

Telnet

Telnet is short for Telecommunications Network, which is a client-side protocol that enables you to access a device over the network.

FTP

File Transfer Protocol (FTP) allows you to upload or download a file or several files to and from a remote location using a client or the command console.

WWW

The World Wide Web allows you to access files hosted in a remote server. For example, you can view text files (usually referred to as ‘pages’) using your web browser via HyperText Transfer Protocol (HTTP).

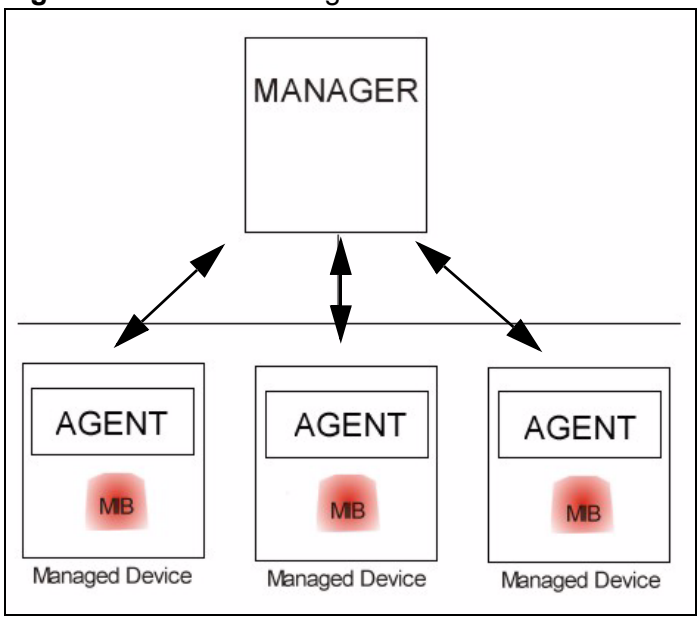
SNMP

Simple Network Management Protocol (SNMP) is a member of the TCP/IP protocol suite used for exchanging management information between network devices.

Your ZyXEL Device supports SNMP agent functionality, which allows a manager station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two (SNMPv2c). The next figure illustrates an SNMP management operation. .

Note: SNMP is only available if TCP/IP is configured.

Figure 49 SNMP Management Mode



An SNMP managed network consists of two main types of component: agents and a manager.

An agent is a management software module that resides in a managed device (the ZyXEL Device). An agent translates the local management information from the managed device into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

SNMP allows a manager and agents to communicate for the purpose of accessing information such as packets received, node port status, etc.

Remote Management Limitations

Remote management over LAN or WLAN will not work when:

- You have disabled that service in one of the remote management screens.
- The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the ZyXEL Device will disconnect the session immediately.

- You may only have one remote management session running at one time. The ZyXEL Device automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows:

1 Telnet

2 HTTP

System Timeout

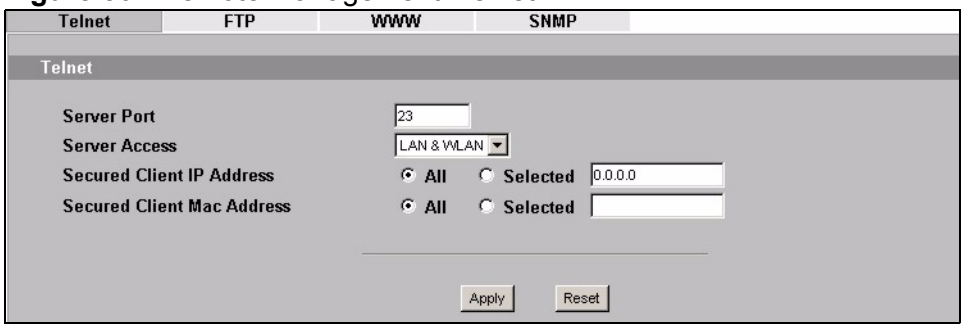
There is a default system management idle timeout of five minutes (three hundred seconds). The ZyXEL Device automatically logs you out if the management session remains idle for longer than this timeout period. The management session does not time out when a statistics screen is polling. You can change the timeout period in the **SYSTEM** screen.

11.4 The Telnet Screen

Use this screen to configure your ZyXEL Device for remote Telnet access. You can use Telnet to access the ZyXEL Device's Command Line Interface (CLI).

Click **REMOTE MGNT** > **TELNET**. The following screen displays.

Figure 50 Remote Management: Telnet



The following table describes the labels in this screen.

Table 29 Remote Management: Telnet

LABEL	DESCRIPTION
TELNET	
Server Port	You can change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using Telnet.

Table 29 Remote Management: Telnet

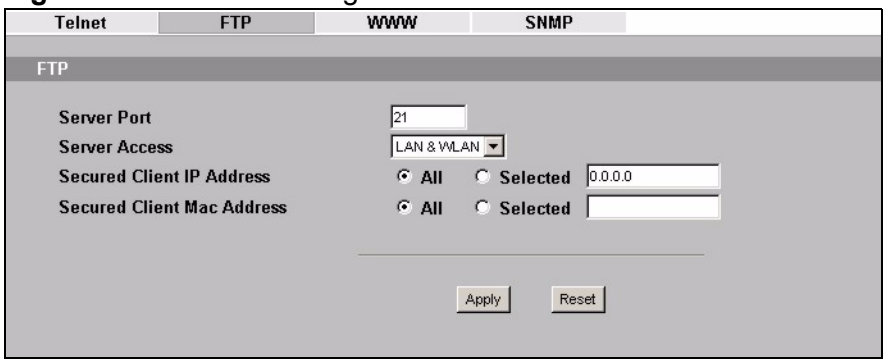
LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.5 The FTP Screen

Use this screen to upload and download the ZyXEL Device's firmware using FTP. To use this feature, your computer must have an FTP client.

To change your ZyXEL Device's FTP settings, click **REMOTE MGMT** > **FTP**. The following screen displays.

Figure 51 Remote Management: FTP



The following table describes the labels in this screen.

Table 30 Remote Management: FTP

LABEL	DESCRIPTION
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.

Table 30 Remote Management: FTP

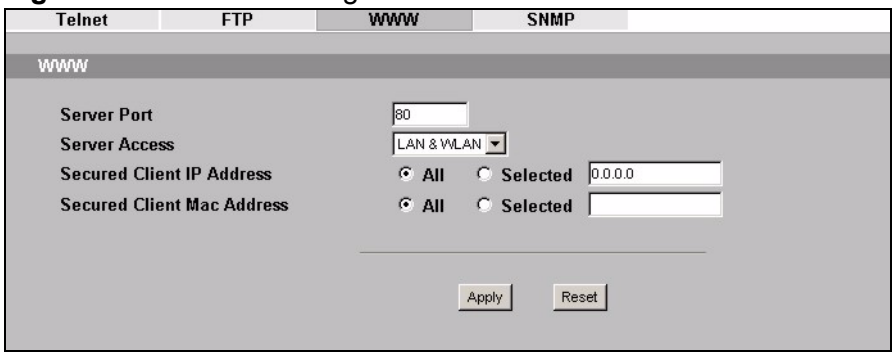
LABEL	DESCRIPTION
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.6 The WWW Screen

Use this screen to configure your ZyXEL Device via the World Wide Web (**WWW)** using a Web browser. This lets you specify which IP addresses or computers are able to communicate with and access the ZyXEL Device.

To change your ZyXEL Device's **WWW** settings, click **REMOTE MGNT** > **WWW**. The following screen shows.

Figure 52 Remote Management: WWW



The following table describes the labels in this screen.

Table 31 Remote Management: WWW

LABEL	DESCRIPTION
WWW	
Server Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

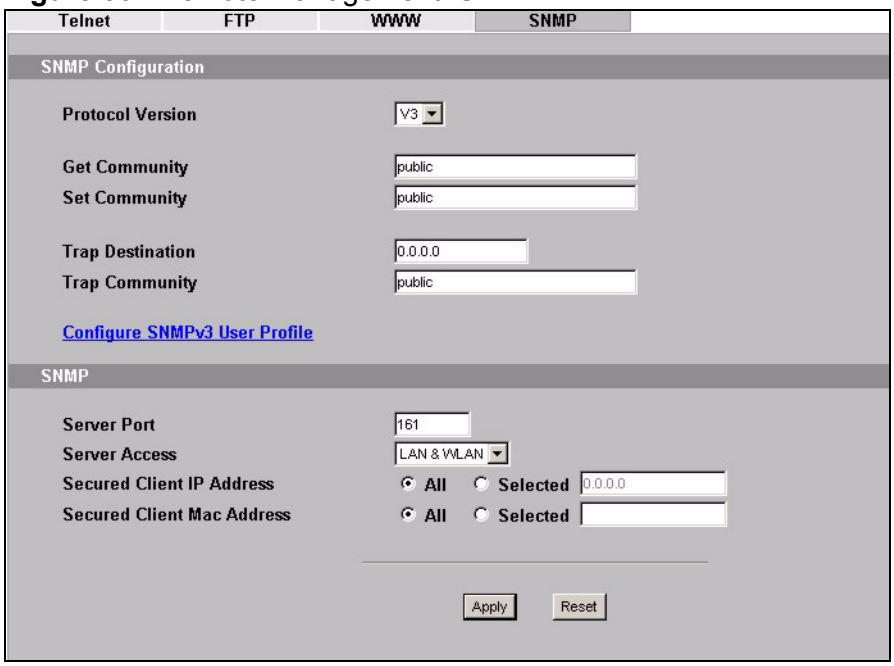
Table 31 Remote Management: WWW

LABEL	DESCRIPTION
Server Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.7 The SNMP Screen

Use this screen to have a manager station administrate your ZyXEL Device over the network. To change your ZyXEL Device's SNMP settings, click **REMOTE MGMT** > **SNMP**. The following screen displays.

Figure 53 Remote Management: SNMP



The following table describes the labels in this screen.

Table 32 Remote Management: SNMP

LABEL	DESCRIPTION
SNMP Configuration	
Get Community	Enter the **Get Community**, which is the password for the incoming Get and GetNext requests from the management station. The default is public and allows all requests.
Set Community	Enter the **Set community**, which is the password for incoming Set requests from the management station. The default is public and allows all requests.
Trap Destination	Type the IP address of the station to send your SNMP traps to.
Trap Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is "public" and allows all requests. This field is available only when **SNMPv1** or **SNMPv2** is selected in the **SNMP Version** field.
Configure SNMPv3 User Profile	Click this to go to the **SNMPv3 User Profile** screen, where you can configure administration and user login details.
SNMP	
Service Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Service Access	Select the interface(s) through which a computer may access the ZyXEL Device using this service.
Secured Client IP Address	A secured client is a "trusted" computer that is allowed to communicate with the ZyXEL Device using this service. Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the IP address that you specify to access the ZyXEL Device using this service.
Secured Client MAC Address	Select **All** to allow any computer to access the ZyXEL Device using this service. Choose **Selected** to just allow the computer with the MAC address that you specify to access the ZyXEL Device using this service.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to begin configuring this screen afresh.

11.8 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

11.8.1 MIB

Managed devices in an SMNP managed network contain object variables or managed objects that define each piece of information to be collected about a device. Examples of variables include such as number of packets received, node port status etc. A Management Information Base (MIB) is a collection of managed objects.SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

- Get - Allows the manager to retrieve an object variable from the agent.
- GetNext - Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
- Set - Allows the manager to set values for object variables within an agent.
- Trap - Used by the agent to inform the manager of some events.

11.8.2 Supported MIBs

The ZyXEL Device supports MIB II that is defined in RFC-1213 and RFC-1215 as well as the proprietary ZyXEL private MIB. The purpose of the MIBs is to let administrators collect statistical data and monitor status and performance.

11.8.3 SNMP Traps

SNMP traps are messages sent by the agents of each managed device to the SNMP manager. These messages inform the administrator of events in data networks handled by the device. The ZyXEL Device can send the following traps to the SNMP manager.

Table 33 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
Generic Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent after booting (power on). This trap is defined in RFC-1215.
warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent after booting (software reboot). This trap is defined in RFC-1215.
linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.

Table 33 SNMP Traps

TRAP NAME	OBJECT IDENTIFIER # (OID)	DESCRIPTION
authenticationFailure (defined in *RFC-1215*)	1.3.6.1.6.3.1.1.5.5	The device sends this trap when it receives any SNMP get or set requirements with the wrong community (password). Note: snmpEnableAuthenTraps, OID 1.3.6.1.2.1.11.30 (defined in RFC 1214 and RFC 1907) must be enabled on in order for the device to send authenticationFailure traps. Use a MIB browser to enable or disable snmpEnableAuthenTraps.
Traps defined in the ZyXEL Private MIB.		
whyReboot	1.3.6.1.4.1.890.1.5.13.0.1	This trap is sent with the reason for restarting before the system reboots (warm start). "System reboot by user!" is added for an intentional reboot (for example, download new files, CI command "sys reboot"). If the system reboots because of fatal errors, a code for the error is listed.
pwTFTPStatus	1.3.6.1.4.1.890.1.9.2.3.3.1	This trap is sent to indicate the status and result of a TFTP client session that has ended.

Some traps include an SNMP interface index. The following table maps the SNMP interface indexes to the ZyXEL Device's physical and virtual ports.

Table 34 SNMP Interface Index to Physical and Virtual Port Mapping

TYPE	INTERFACE	PORT
Physical	enet0	Wireless LAN adaptor WLAN1
	enet1	Ethernet port (LAN)
	enet2	Wireless LAN adaptor WLAN2
Virtual	enet3 ~ enet9	WLAN1 in MBSSID mode
	enet10 ~ enet16	WLAN2 in MBSSID mode
	enet17 ~ enet21	WLAN1 in WDS mode
	enet22 ~ enet26	WLAN2 in WDS mode

12

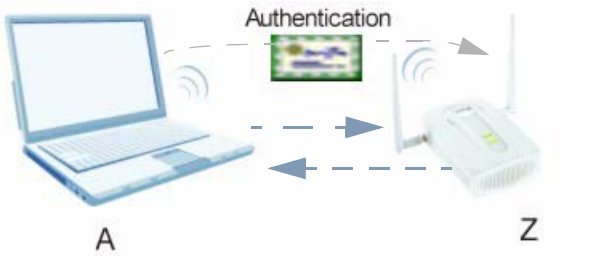
Certificate Screen

12.1 Overview

This chapter describes how your ZyXEL Device can use certificates as a means of authenticating wireless clients. It gives background information about public-key certificates and explains how to use them.

A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Figure 54 Certificates Example



In the figure above, the ZyXEL Device (Z) checks the identity of the notebook (A) using a certificate before granting access to the network.

12.2 What You Can Do in the Certificate Screen

Use the **CERTIFICATES > Certificate** screen (seen Section 12.4 on page 112) to view, delete and import certificates.

12.3 What You Need To Know About Certificates

The certification authority certificate that you can import to your ZyXEL Device should be in PFX PKCS#12 file format. This format referred to as the Personal Information Exchange Syntax Standard is comprised of a private key-public certificate pair that is further encrypted with a password. Before you import a

certificate into the ZyXEL Device, you should verify that you have the correct certificate.

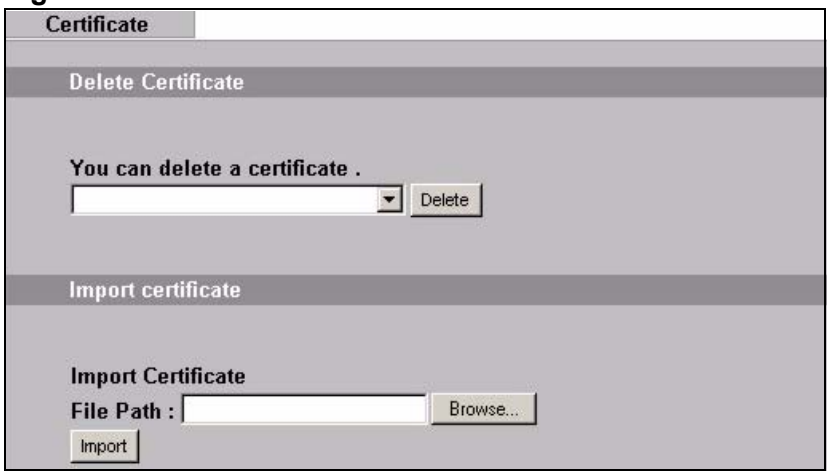
Key distribution is simple and very secure since you can freely distribute public keys and you never need to transmit private keys.

12.4 Certificate Screen

Use this screen to view, delete and import certificates.

Click **CERTIFICATE** to open the ZyXEL Device's summary list of certificates and to import a new certificate. See the following figure.

Figure 55 Certificate



The following table describes the labels in this screen.

Table 35 Certificate

LABEL	DESCRIPTION
Delete Certificate	
You can delete a certificate	Select the certificate from the list that you want to delete.
Delete	Click this to delete the selected certificate.
Import Certificate	
File Path	Enter the location of a previously-saved certificate to upload to the ZyXEL Device. Alternatively, click the **Browse** button to locate a list.
Browse	Click this button to locate a previously-saved certificate to upload to the ZyXEL Device.
Import	Click this button to upload the previously-saved certificate displayed in the **File Path** field to the ZyXEL Device.

12.5 Technical Reference

This section provides technical background information about the topics covered in this chapter.

12.5.1 Private-Public Certificates

When using public-key cryptology for authentication, each host has two keys. One key is public and can be made openly available. The other key is private and must be kept secure.

These keys work like a handwritten signature (in fact, certificates are often referred to as "digital signatures"). Only you can write your signature exactly as it should look. When people know what your signature looks like, they can verify whether something was signed by you, or by someone else. In the same way, your private key "writes" your digital signature and your public key allows people to verify whether data was signed by you, or by someone else. This process works as follows.

1. Tim wants to send a message to Jenny. He needs her to be sure that it comes from him, and that the message content has not been altered by anyone else along the way. Tim generates a public key pair (one public key and one private key).
2. Tim keeps the private key and makes the public key openly available. This means that anyone who receives a message seeming to come from Tim can read it and verify whether it is really from him or not.
3. Tim uses his private key to sign the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to verify it. Jenny knows that the message is from Tim, and that although other people may have been able to read the message, no-one can have altered it (because they cannot re-sign the message with Tim's private key).
5. Additionally, Jenny uses her own private key to sign a message and Tim uses Jenny's public key to verify the message.

12.5.2 Certification Authorities

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the ZyXEL Device to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

12.5.3 Checking the Fingerprint of a Certificate on Your Computer

A certificate's fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to check a certificate's fingerprint to verify that you have the actual certificate.

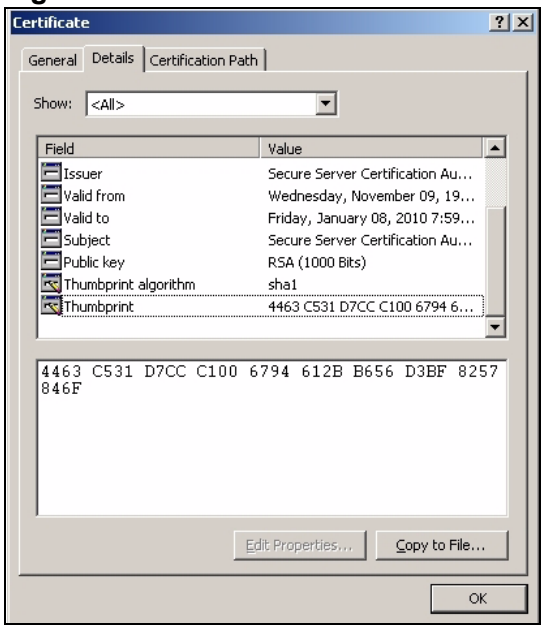
1 Browse to where you have the certificate saved on your computer.

2 Make sure that the certificate has a ".cer" or ".crt" file name extension.

Figure 56 Certificates on Your Computer

3 Double-click the certificate's icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 57 Certificate Details



4 Use a secure method to verify that the certificate owner has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields. The secure method may vary according to your situation. Possible examples would be over the telephone or through an HTTPS connection.

13

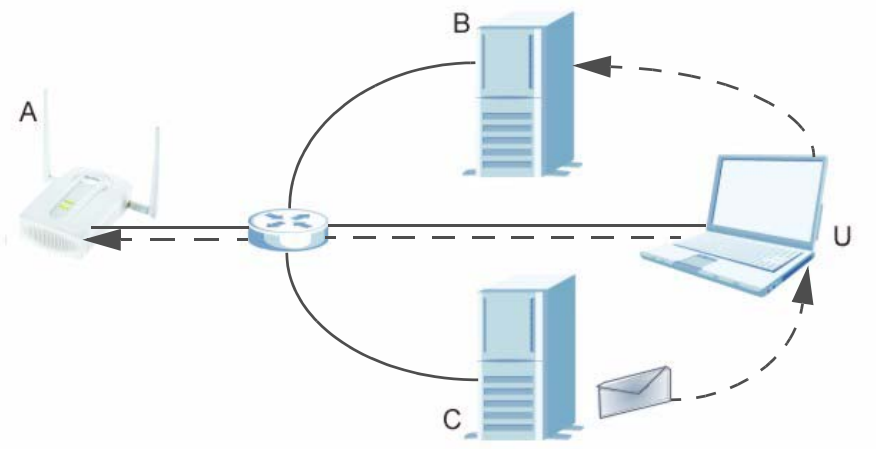
Log Screens

13.1 Overview

This chapter provides information on viewing and generating logs on your ZyXEL Device.

Logs are files that contain recorded network activity over a set period. They are used by administrators to monitor the health of the system(s) they are managing. Logs enable administrators to effectively monitor events, errors, progress, etc. so that when network problems or system failures occur, the cause or origin can be traced. Logs are also essential for auditing and keeping track of changes made by users.

Figure 58 Accessing Logs in the Network



The figure above illustrates three ways to access logs. The user **(U)** can access logs directly from the ZyXEL Device **(A)** via the Web configurator. Logs can also be located in an external log server **(B)**. An email server **(C)** can also send harvested logs to the user's email account.

13.2 What You Can Do in the Log Screens

- Use the **View Log** screen (Section 13.4 on page 116) to display all logs or logs for a certain category. You can view logs and alert messages in this page. Once the log entries are all used, the log will wrap around and the old logs will be deleted.
- Use the **Log Settings** screen (Section 13.5 on page 117) to configure where and when the ZyXEL Device will send the logs, and which logs and/or immediate alerts it will send.

13.3 What You Need To Know About Logs

Alerts and Logs

An alert is a type of log that warrants more serious attention. Some categories such as **System Errors** consist of both logs and alerts. You can differentiate them by their color in the **View Log** screen. Alerts are displayed in red and logs are displayed in black.

Receiving Logs via E-mail

If you want to receive logs in your e-mail account, you need to have the necessary details ready, such as the Server Name or Simple Mail Transfer Protocol (SMTP) Address of your e-mail account. Ensure that you have a valid e-mail address.

Enabling Syslog Logging

To enable Syslog Logging, obtain your Syslog server's IP address (or server name).

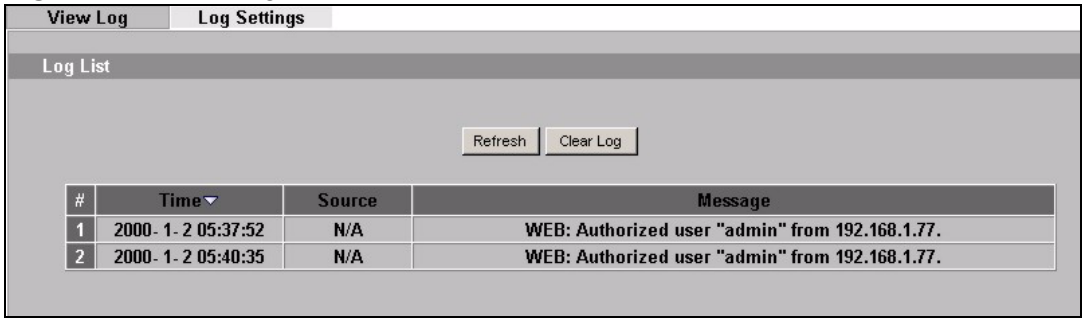
13.4 View Log Screen

Use this screen to view all the ZyXEL Device's logs in one location.

Click **Logs > View Log**. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see Figure 60 on page 118). Options include logs about system maintenance, system errors and access control.

Click a column heading to sort the entries. A triangle indicates the direction of the sort order.

Figure 59 View Log


View Log
Log Settings
Log List
Refresh
Clear Log
Time Source Message
1 2000-1-2 05:37:52 N/A WEB: Authorized user "admin" from 192.168.1.77.
2 2000-1-2 05:40:35 N/A WEB: Authorized user "admin" from 192.168.1.77.

The following table describes the labels in this screen.

Table 36 View Log

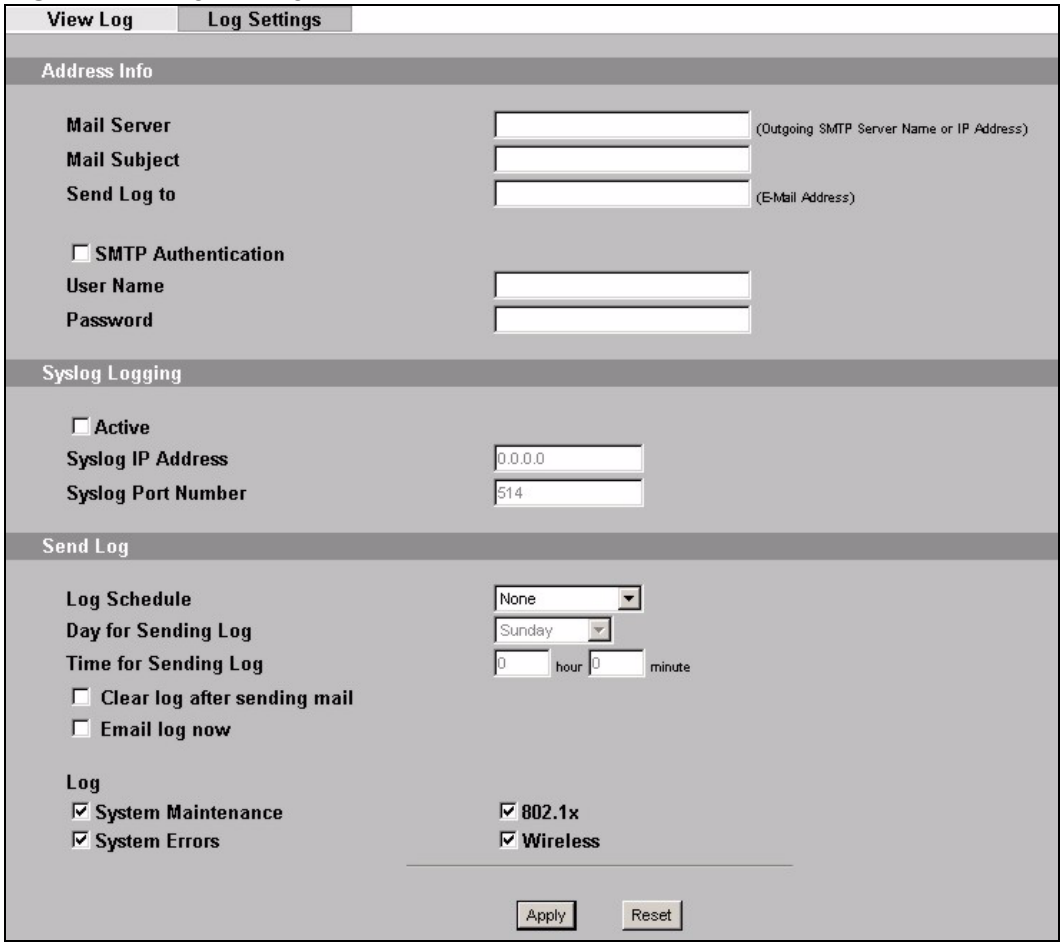
LABEL	DESCRIPTION
Time	This field displays the time the log was recorded.
Source	This field lists the source IP address and the port number of the incoming packet.
Message	This field states the reason for the log.
Refresh	Click **Refresh** to renew the log screen.
Clear Log	Click **Clear Log** to clear all the logs.

13.5 Log Settings Screen

Use this screen to configure to where and when the ZyXEL Device is to send the logs and which logs and/or immediate alerts it is to send.

To change your ZyXEL Device's log settings, click **LOGS** > **Log Settings**. The screen appears as shown.

Figure 60 Log Settings



The following table describes the labels in this screen.

Table 37 Log Settings

LABEL	DESCRIPTION
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages will not be sent via e-mail.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the ZyXEL Device sends.
Send Log to	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs will not be sent via e-mail.
SMTP Authentication	If you use SMTP authentication, the mail receiver should be the owner of the SMTP account.
User Name	If your e-mail account requires SMTP authentication, enter the username here.
Password	Enter the password associated with the above username.

Table 37 Log Settings

LABEL	DESCRIPTION
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click **Active** to enable syslog logging.
Syslog IP Address	Enter the IP address of the syslog server that will log the selected categories of logs.
Syslog Port Number	Enter the port number of the syslog server that will log the selected categories of logs.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as E-mail: • Daily • Weekly • Hourly • When Log is Full • None. If the **Weekly** or the **Daily** option is selected, specify a time of day when the E-mail should be sent. If the **Weekly** option is selected, then also specify which day of the week the E-mail should be sent. If the **When Log is Full** option is selected, an alert is sent when the log fills up. If you select **None**, no log messages are sent.
Day for Sending Log	This field is only available when you select **Weekly** in the **Log Schedule** field. Use the drop down list box to select which day of the week to send the logs.
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 pm) to send the logs.
Clear log after sending mail	Select the check box to clear all logs after logs and alert messages are sent via e-mail.
Email log now	Select the categories of alerts for which you want the ZyXEL Device to immediately send e-mail alerts.
Log	
System Maintenance	Click this to receive logs related to system maintenance.
System Errors	Click this to receive logs related to system errors.
802.1x	Click this to receive logs related to the 802.1x mode.
Wireless	Click this to receive logs related to the wireless function.
Apply	Click **Apply** to save your customized settings and exit this screen.
Reset	Click **Reset** to reconfigure all the fields in this screen.

13.6 Technical Reference

This section provides some technical background information about the topics covered in this chapter.

13.6.1 Example Log Messages

The following tables provide descriptions of some example log messages that the ZyXEL Device generates.

Table 38 System Maintenance Logs

LOG MESSAGE	DESCRIPTION
WLAN: Radar interference 2412 MHz.	Wireless driver receives radar pulse at center frequency 2412 MHz.
WLAN: CW interference 2412 MHz.	Wireless driver receives noise interference pulse at center frequency 2412 MHz.
WLAN service started.	Wireless port ath0 started.
WLAN service stopped.	Wireless port ath0 stopped.
AP MIC failed.	Wireless driver MIC checked failed.
AP MIC attacked.	Wireless driver received MIC attack packet.
Station authenticated.	AP received the request for authentication from station and authenticated the station successfully.
Station authentication failed.	AP received the request for authentication from station but the authentication failed.
Station deauthenticated.	AP receive the deauthenticated packet from the STA which connected with AP.
Station associated.	AP receive the association request packet from the STA which connected with AP.
Station disassociated.	AP receive the disassociation request packet from the STA, which connected with AP.
Station refused.	A STA wanted to connect to the AP but was refused.
Remote Bridge AP configured.	Remote AP MAC address was configured.
Remote Bridge AP deleted.	Remote AP MAC address was deleted.
CLI: Authorized user from IP.	A device succesfully logs into the AP via Telnet (the device's IP address shows in the log message.)
CLI: Unauthorized user from IP.	A device fails to log into the AP via Telnet (the device's IP address shows in the log message.)
WEB: Authorized user from IP.	A device successfully logs into the AP via WWW (the device's IP address shows in the log message.)
WEB: Unauthorized user from IP.	A device fails to log into the AP via WWW (the device's IP address shows in the log message.)

13.7 Log Commands

Go to the command interpreter interface (refer to Appendix I on page 199 for the Command Interpreter appendix explains how to access and use the commands).

13.7.1 Configuring What You Want the ZyXEL Device to Log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the ZyXEL Device is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record

Table 39 Log Categories and Available Settings

LOG CATEGORIES	AVAILABLE PARAMETERS
error	0, 1, 2, 3
mten	0, 1
Use `0` to not record logs for that category, `1` to record only logs for that category, `2` to record only alerts for that category, and `3` to record both logs and alerts for that category.	

Use the `sys logs save` command to store the settings in the ZyXEL Device (you must do this in order to record logs).

13.7.2 Displaying Logs

Use the `sys logs display` command to show all of the logs in the ZyXEL Device's log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual ZyXEL Device log category.

Use the `sys logs clear` command to erase all of the ZyXEL Device's logs.

13.7.3 Command List

The following table provides the commands that can be used for your ZyXEL Device to configure the log settings.

Table 40 Log Command List

KEYWORD	DESCRIPTION
`client`	Enable SYSLOG client
`ipaddr`	SYSLOG server IP address
`port`	SYSLOG server port
`Email server`	E-mail server address
`Email subject`	E-mail subject
`Email Address`	E-mail address

KEYWORD	DESCRIPTION
Email SmtpAuthEnable	SMPTP auth enable when e-mail log
Email User	E-mail user name
Email Password	E-mail password
Email Schedule	E-mail schedule mode
Email Day	E-mail schedule day
Email Hour	E-mail schedule hour
Email Minute	E-mail schedule minute
Email Clear	Clear log after e-mail
Email Now	Send e-mail now

14 Maintenance

14.1 Overview

This chapter describes the maintenance screens. It discusses how you can view the association list and channel usage, upload new firmware, manage configuration and restart your ZyXEL Device without turning it off and on.

14.2 What You Can Do in the Maintenance Screens

- Use the **Association List** screen (see Section 14.4 on page 124) to view the wireless stations that are currently associated with the ZyXEL Device.
- Use the **Channel Usage** screen (see Section 14.5 on page 124) to view whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.
- Use the **F/W Upload** screen (see Section 14.6 on page 126) to upload the latest firmware for your ZyXEL Device.
- Use the **Configuration** screen (see Section 14.7 on page 127) to view information related to factory defaults, backup configuration, and restoring configuration.
- Use **Restart** screen (see Section 14.8 on page 130) to reboot the ZyXEL Device without turning the power off.

14.3 What You Need To Know About the Maintenance Screens

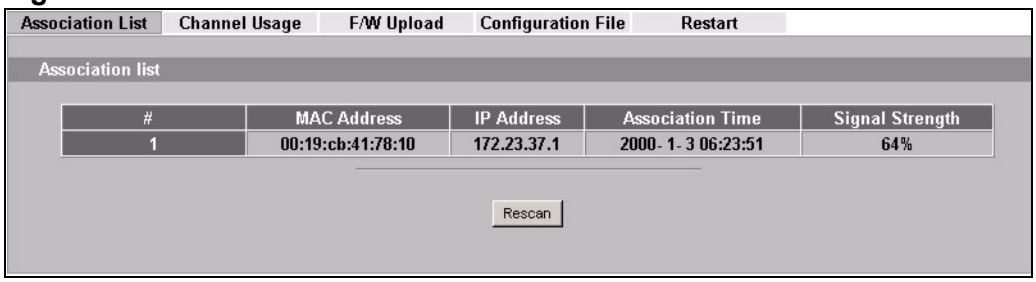
You can find the firmware for your device at www.zyxel.com. It is a file that (usually) uses the system model name with a "*.bin" extension, for example "NWA-1100.bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

14.4 Association List Screen

Use this screen to view the wireless stations that are currently associated with the ZyXEL Device.

Click **Maintenance** > **Association List**. The following screen displays.

Figure 61 Association List



The following table describes the labels in this screen.

Table 41 Association List

LABEL	DESCRIPTION
#	This is the index number of an associated wireless station.
MAC Address	This field displays the MAC address of an associated wireless station.
IP Address	This identifies the individual devices on a network.
Association Time	This field displays the time a wireless station first associated with the ZyXEL Device.
Signal Strength	This field displays the RSSI (Received Signal Strength Indicator) of the wireless connection.
Rescan	Click **Rescan** to reload the screen.

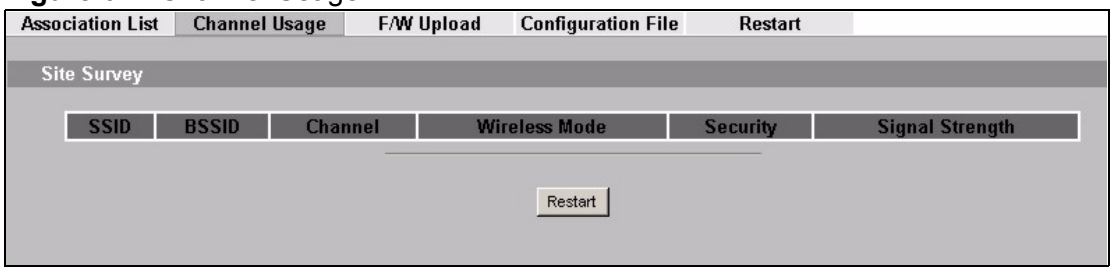
14.5 Channel Usage Screen

Use this screen to know whether a channel is used by another wireless network or not. If a channel is being used, you should select a channel removed from it by five channels to completely avoid overlap.

Click **Maintenance** > **Channel Usage** to display the screen shown next.

Wait a moment while the ZyXEL Device compiles the information.

Figure 62 Channel Usage



The following table describes the labels in this screen.

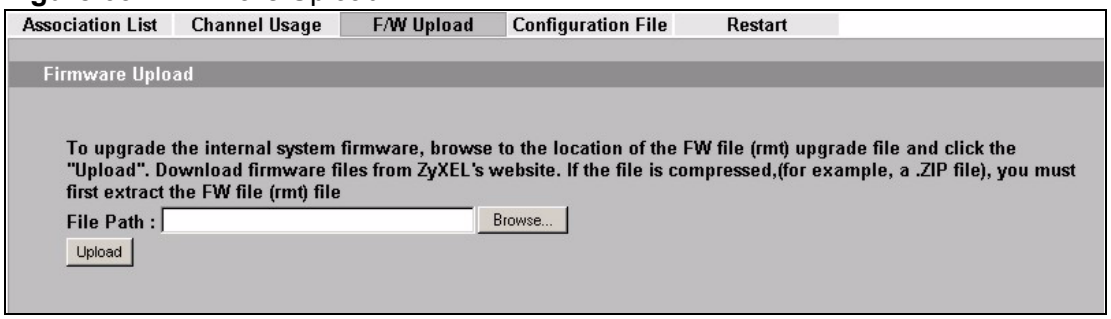
Table 42 Channel Usage

LABEL	DESCRIPTION
SSID	This is the Service Set IDentification name of the AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network. For our purposes, we define an Infrastructure network as a wireless network that uses an AP and an Ad-Hoc network (also known as Independent Basic Service Set (IBSS)) as one that doesn't. See the chapter on wireless configuration for more information on basic service sets (BSS) and extended service sets (ESS).
BSSID	This field displays the MAC address of the AP in an Infrastructure wireless network. It is randomly generated (so ignore it) in an Ad-Hoc wireless network.
Channel	This is the index number of the channel currently used by the associated AP in an Infrastructure wireless network or wireless station in an Ad-Hoc wireless network.
Wireless Mode	This is the IEEE 802.1x standard used by your ZyXEL Device to apply enhanced security methods for both the authentication of wireless stations and encryption key management.
Security	This is the wireless security method used by your ZyXEL Device protect wireless communication between wireless stations, access points and the wired network.
Restart	Click **Restart** to reload the screen.

14.6 F/W Upload Screen

Use this screen to upload a firmware to your ZyXEL Device. Click **Maintenance** > **F/W Upload**. Follow the instructions in this section to upload firmware to your ZyXEL Device.

Figure 63 Firmware Upload


Association List
Channel Usage
F/W Upload
Configuration File
Restart
Firmware Upload
To upgrade the internal system firmware, browse to the location of the FW file (rmt) upgrade file and click the "Upload". Download firmware files from ZyXEL's website. If the file is compressed,(for example, a .ZIP file), you must first extract the FW file (rmt) file
File Path :
Browse...
Upload

The following table describes the labels in this screen.

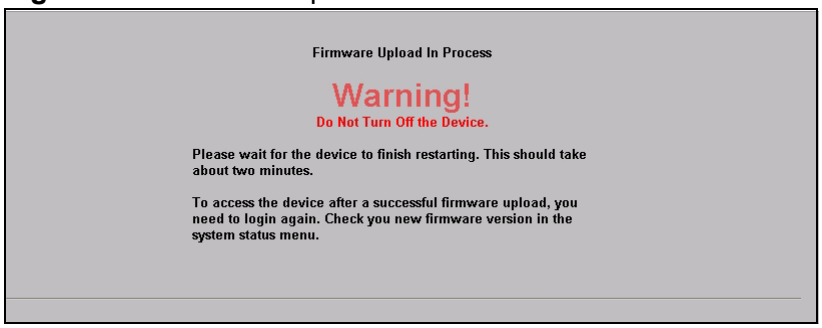
Table 43 Firmware Upload

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.

Do not turn off the ZyXEL Device while firmware upload is in progress!

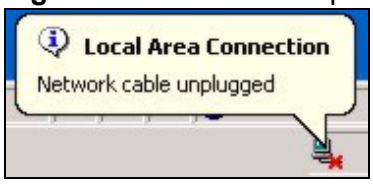
After you see the **Firmware Upload in Process** screen, wait two minutes before logging into the ZyXEL Device again.

Figure 64 Firmware Upload In Process


Firmware Upload In Process
Warning!
Do Not Turn Off the Device.
Please wait for the device to finish restarting. This should take about two minutes.
To access the device after a successful firmware upload, you need to login again. Check you new firmware version in the system status menu.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

Figure 65 Network Temporarily Disconnected



After two minutes, log in again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **F/W Upload** screen.

Figure 66 Firmware Upload Error

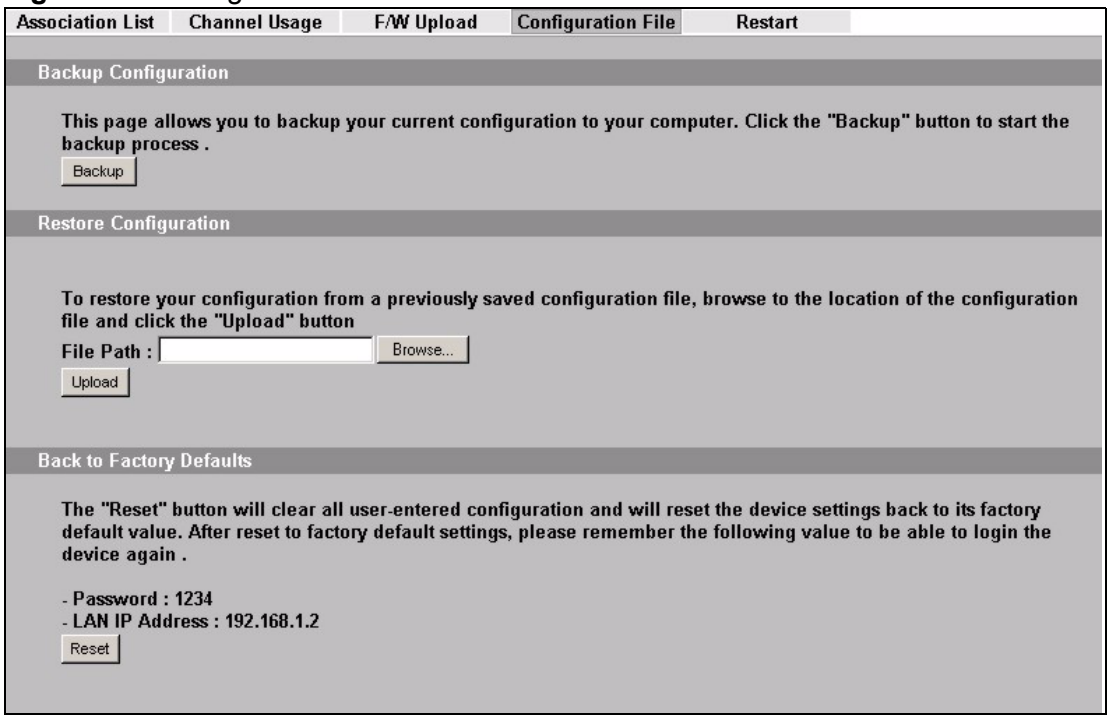
Firmware upload error!
The uploaded file was not accepted by the router. Please return to the previous page and select a valid upgrade file. Click Help for more information.
Return

14.7 Configuration Screen

Use this screen to backup, restore and reset the configuration of your ZyXEL Device.

Click **Maintenance** > **Configuration**. The screen appears as shown next.

Figure 67 Configuration


Association List
Channel Usage
F/W Upload
Configuration File
Restart
Backup Configuration
This page allows you to backup your current configuration to your computer. Click the "Backup" button to start the backup process .
Backup
Restore Configuration
To restore your configuration from a previously saved configuration file, browse to the location of the configuration file and click the "Upload" button
File Path :
Browse...
Upload
Back to Factory Defaults
The "Reset" button will clear all user-entered configuration and will reset the device settings back to its factory default value. After reset to factory default settings, please remember the following value to be able to login the device again .
- Password : 1234
- LAN IP Address : 192.168.1.2
Reset

14.7.1 Backup Configuration

Backup configuration allows you to back up (save) the ZyXEL Device's current configuration to a file on your computer. Once your ZyXEL Device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Click **Backup** to save the ZyXEL Device's current configuration to your computer.

14.7.2 Restore Configuration

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your ZyXEL Device.

Table 44 Restore Configuration

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse ...** to find it.

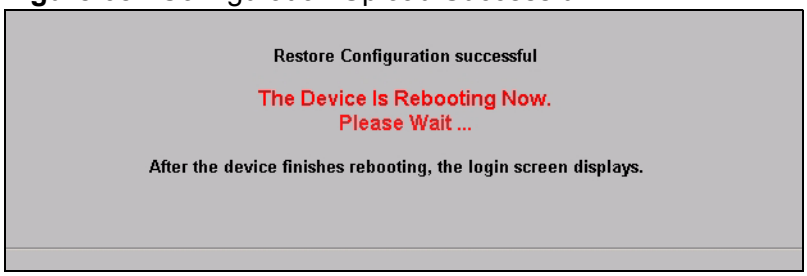
Table 44 Restore Configuration

LABEL	DESCRIPTION
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process.

Do not turn off the ZyXEL Device while configuration file upload is in progress.

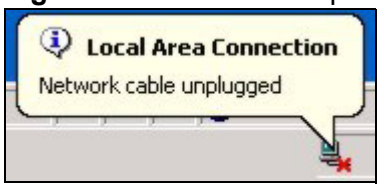
After you see a "restore configuration successful" screen, you must then wait one minute before logging into the ZyXEL Device again.

Figure 68 Configuration Upload Successful


Restore Configuration successful
The Device Is Rebooting Now.
Please Wait ...
After the device finishes rebooting, the login screen displays.

The ZyXEL Device automatically restarts in this time causing a temporary network disconnect. In some operating systems, you may see the following icon on your desktop.

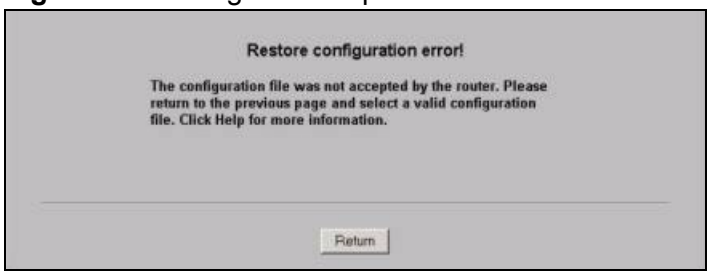
Figure 69 Network Temporarily Disconnected



If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default ZyXEL Device IP address (192.168.1.2). See your Quick Start Guide for details on how to set up your computer's IP address.

If the upload was not successful, the following screen will appear. Click **Return** to go back to the **Configuration** screen.

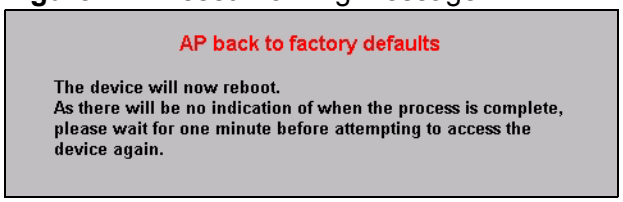
Figure 70 Configuration Upload Error


Restore configuration error!
The configuration file was not accepted by the router. Please return to the previous page and select a valid configuration file. Click Help for more information.
Return

14.7.3 Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the ZyXEL Device to its factory defaults as shown on the screen. The following warning screen will appear.

Figure 71 Reset Warning Message


AP back to factory defaults
The device will now reboot.
As there will be no indication of when the process is complete, please wait for one minute before attempting to access the device again.

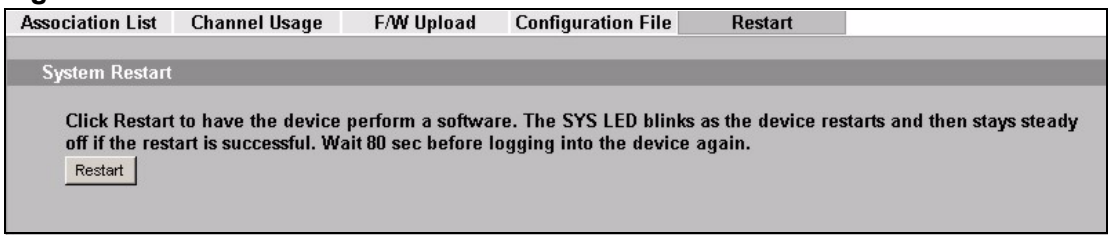
You can also press the **RESET** button to reset your ZyXEL Device to its factory default settings. Refer to Section 2.2 on page 30 for more information.

14.8 Restart Screen

Use this screen to reboot the ZyXEL Device without turning the power off.

Click **Maintenance** > **Restart**. The following screen displays.

Figure 72 Restart Screen


Association List
Channel Usage
F/W Upload
Configuration File
Restart
System Restart
Click Restart to have the device perform a software. The SYS LED blinks as the device restarts and then stays steady off if the restart is successful. Wait 80 sec before logging into the device again.
Restart

Click **Restart** to have the ZyXEL Device reboot. This does not affect the ZyXEL Device's configuration.

15

Troubleshooting

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- ZyXEL Device Access and Login
- Internet Access

15.1 Power, Hardware Connections, and LEDs

The ZyXEL Device does not turn on. None of the LEDs turn on.

1. Make sure you are using the power adaptor or cord included with the ZyXEL Device.
2. Make sure the power adaptor or cord is connected to the ZyXEL Device and plugged in to an appropriate power source. Make sure the power source is turned on.
3. Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.
4. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.7 on page 27.
2. Check the hardware connections. See the Quick Start Guide.

3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.

4 Disconnect and re-connect the power adaptor to the ZyXEL Device.

5 If the problem continues, contact the vendor.

15.2 ZyXEL Device Access and Login

I forgot the IP address for the ZyXEL Device.

1 The default IP address is **192.168.1.2**.

2 If you changed the IP address and have forgotten it, you might get the IP address of the ZyXEL Device by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter "**cmd**", and then enter "**ipconfig**". The IP address of the **Default Gateway** might be the IP address of the ZyXEL Device (it depends on the network), so enter this IP address in your Internet browser.

3 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

I forgot the password.

1 The default password is **1234**.

2 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

I cannot see or access the **Login** screen in the web configurator.

1 Make sure you are using the correct IP address.

- The default IP address is 192.168.1.2.
- If you changed the IP address (Section 10.4 on page 98), use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the ZyXEL Device.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 27.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Section 15.1 on page 131.

4 Make sure your computer is in the same subnet as the ZyXEL Device. (If you know that there are routers between your computer and the ZyXEL Device, skip this step.)

- If there is no DHCP server on your network, make sure your computer's IP address is in the same subnet as the ZyXEL Device.

5 Reset the device to its factory defaults, and try to access the ZyXEL Device with the default IP address. See your Quick Start Guide.

6 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the ZyXEL Device using another service, such as Telnet. If you can access the ZyXEL Device, check the remote management settings to find out why the ZyXEL Device does not respond to HTTP.
- If your computer is connected to the **WAN** port or is connected wirelessly, use a computer that is connected to a **LAN**/**ETHERNET** port.

I can see the **Login** screen, but I cannot log in to the ZyXEL Device.

1 Make sure you have entered the user name and password correctly. The default password is **1234**. This fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using the Telnet to access the ZyXEL Device. Log out of the ZyXEL Device in the other session, or ask the person who is logged in to log out.

3 Disconnect and re-connect the power adaptor or cord to the ZyXEL Device.

4 If this does not work, you have to reset the device to its factory defaults. See Section 2.2 on page 30.

I cannot use FTP to upload new firmware.

See the troubleshooting suggestions for I cannot see or access the Login screen in the web configurator. Ignore the suggestions about your browser.

15.3 Internet Access

I cannot access the Internet.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 15.1 on page 131.
2. 2. Make sure your ZyXEL Device is connected to a networking device that provides Internet access.
3. If you are trying to access the Internet wirelessly, make sure the wireless settings on the wireless client are the same as the settings on the AP.
4. Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.
5. If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the ZyXEL Device), but my Internet connection is not available anymore.

1. Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.7 on page 27.
2. Reboot the ZyXEL Device.
3. If the problem continues, contact your ISP or network administrator.

The Internet connection is slow or intermittent.

1. There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.7 on page 27. If the ZyXEL Device is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2. Check the signal strength. If the signal is weak, try moving the ZyXEL Device (in wireless client mode) closer to the AP (if possible), and look around to see if there are any devices that might be interfering with the wireless network (microwaves, other wireless networks, and so on).

3. Reboot the ZyXEL Device.

4. If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

   Advanced Suggestions

   - Check the settings for QoS. If it is disabled, you might consider activating it.

PART III Appendices and Index

Product Specifications (139)

Power over Ethernet (PoE) Specifications (141)

Power Adaptor Specifications (143)

Setting up Your Computer's IP Address (145)

Wireless LANs (157)

Pop-up Windows, JavaScripts and Java Permissions (173)

IP Addresses and Subnetting (181)

Text File Based Auto Configuration (191)

How to Access and Use the CLI (199)

Open Software Announcements (203)

Legal Information (215)

Index (219)

A

Product Specifications

The following tables summarize the ZyXEL Device's hardware and firmware features.

Table 45 Hardware Specifications

Power Specification	12 V DC, 1 A
Reset button	Returns all settings to their factory defaults.
Ethernet Port	• Auto-negotiating: 10 Mbps or 100 Mbps in either half-duplex or full-duplex mode. • Auto-crossover: Use either crossover or straight-through Ethernet cables.
Power over Ethernet (PoE)	IEEE 802.3af compliant.
Antenna	SMA antenna connectors, equipped by default with 3dBi omni antenna, 60°
Operation Temperature	0 ~ 50 º C
Storage Temperature	-30 ~ 60 º C
Operation Humidity	20 ~ 90 % (non-condensing)
Storage Humidity	10 ~ 90 % (non-condensing)
Dimensions	152mm x 92mm x 45mm

Table 46 Firmware Specifications

Default IP Address	192.168.1.2
Default Subnet Mask	255.255.255.0 (24 bits)
Default Password	1234
Wireless LAN Standards	IEEE 802.11b, IEEE 802.11g
Wireless security	WEP, WPA(2), WPA(2)-PSK, 802.1x
STP (Spanning Tree Protocol) / RSTP (Rapid STP)	(R)STP detects and breaks network loops and provides backup links between switches, bridges or routers. It allows a bridge to interact with other (R)STP-compliant bridges in your network to ensure that only one path exists between any two stations on the network.
WMM QoS	WMM (Wi-Fi MultiMedia) QoS (Quality of Service) allows you to prioritize wireless traffic.

Table 46 Firmware Specifications

Certificates	The ZyXEL Device can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.
SSL Passthrough	SSL (Secure Sockets Layer) uses a public key to encrypt data that's transmitted over an SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https" instead of "http". The ZyXEL Device allows SSL connections to take place through the ZyXEL Device.
MAC Address Filter	Your ZyXEL Device checks the MAC address of the wireless station against a list of allowed or denied MAC addresses.
Wireless Association List	With the wireless association list, you can see the list of the wireless stations that are currently using the ZyXEL Device to access your wired network.
Logging and Tracing	Built-in message logging and packet tracing.
Embedded FTP and TFTP Servers	The embedded FTP and TFTP servers enable fast firmware upgrades as well as configuration file backups and restoration.
Auto Configuration	Administrators can use text configuration files to configure the wireless LAN settings for multiple APs. The AP can automatically get a configuration file from a TFTP server at start up or after renewing DHCP client information.
SNMP	SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your ZyXEL Device supports SNMP agent functionality, which allows a manger station to manage and monitor the ZyXEL Device through the network. The ZyXEL Device supports SNMP version one (SNMPv1) and version two c (SNMPv2c).

B

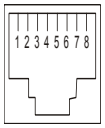
Power over Ethernet (PoE) Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.-7

Table 47 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Table 48 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

C

Power Adaptor Specifications

Table 49 North American Plug Standards

AC Power Adaptor Model	ADS6818-1812-W 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5A, 18W
Power Consumption	6 W Max
Safety Standards	UL, CUL (UL60950 Third Edition, CSA C22.2 No. 60950)

Table 50 European Plug Standards

AC Power Adaptor Model	ADS6818-1812-B 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS, CE (EN 60950)

Table 51 United Kingdom Plug Standards

AC Power Adaptor Model	ADS6818-1812-D 1215
Input Power	100~240 Volts AC, 50~60 Hz,0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	TUV-GS (BS EN 60950)

Table 52 Australia and New Zealand Plug Standards

AC Power Adaptor Model	ADS6818-1812-A 1215
Input Power	100~240 Volts AC, 50~60 Hz, 0.5 A
Output Power	12 Volts DC, 1.5 A, 18 W
Power Consumption	6 W Max
Safety Standards	DOFT (AS/NZS 60950, AS/NZSB 3112:1-2)

D

Setting up Your Computer's IP Address

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

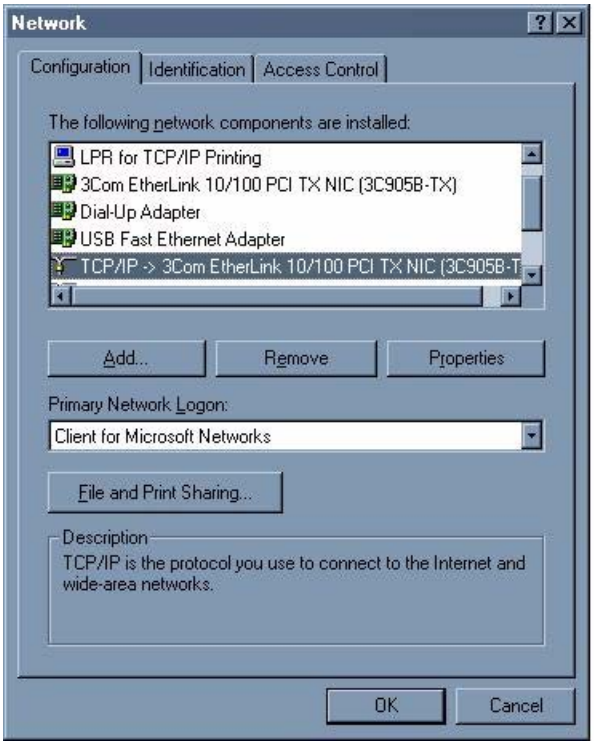
After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as the ZyXEL Device's LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window

Figure 73 WIndows 95/98/Me: Network: Configuration



Installing Components

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

1 In the **Network** window, click **Add**.

2 Select **Adapter** and then click **Add**.

3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

1 In the **Network** window, click **Add**.

2 Select **Protocol** and then click **Add**.

3 Select **Microsoft** from the list of **manufacturers**.

4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

1 Click **Add**.

2 Select **Client** and then click **Add**.

3 Select **Microsoft** from the list of manufacturers.

4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

5 Restart your computer so the changes you made take effect.

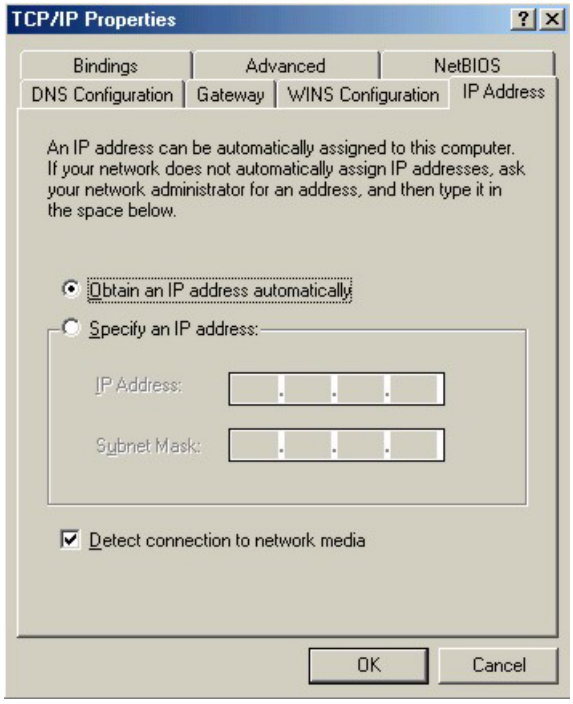
Configuring

1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**

2 Click the **IP Address** tab.

- If your IP address is dynamic, select **Obtain an IP address automatically**.
- If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.

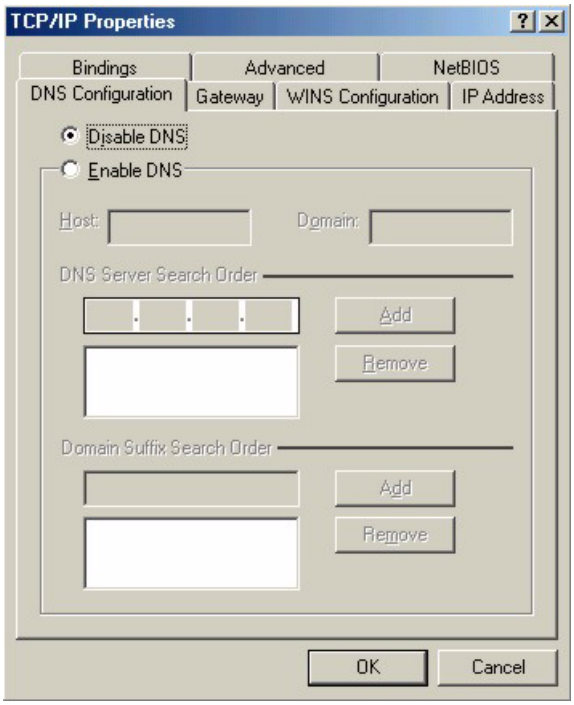
Figure 74 Windows 95/98/Me: TCP/IP Properties: IP Address


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
Detect connection to network media
OK
Cancel

3 Click the **DNS** Configuration tab.

- If you do not know your DNS information, select **Disable DNS**.
- If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).

Figure 75 Windows 95/98/Me: TCP/IP Properties: DNS Configuration



4 Click the **Gateway** tab.

- If you do not know your gateway's IP address, remove previously installed gateways.
- If you have a gateway IP address, type it in the **New gateway field** and click **Add**.

5 Click **OK** to save and close the **TCP/IP Properties** window.

6 Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

7 Turn on your ZyXEL Device and restart your computer when prompted.

Verifying Settings

1 Click **Start** and then **Run**.

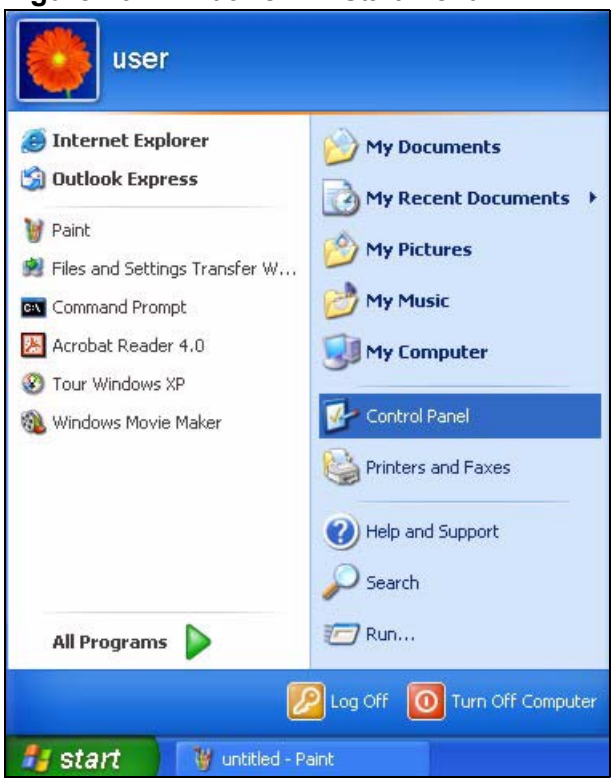
2 In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.

3 Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 76 Windows XP: Start Menu

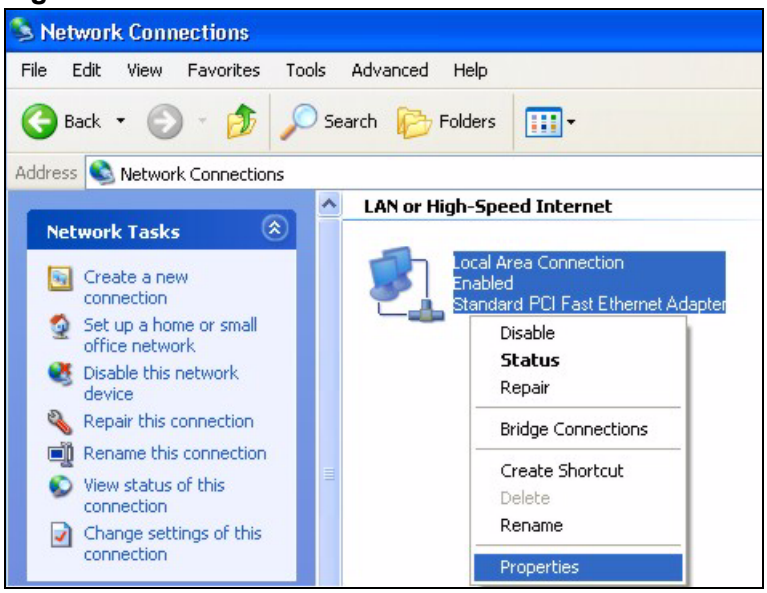


2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 77 Windows XP: Control Panel

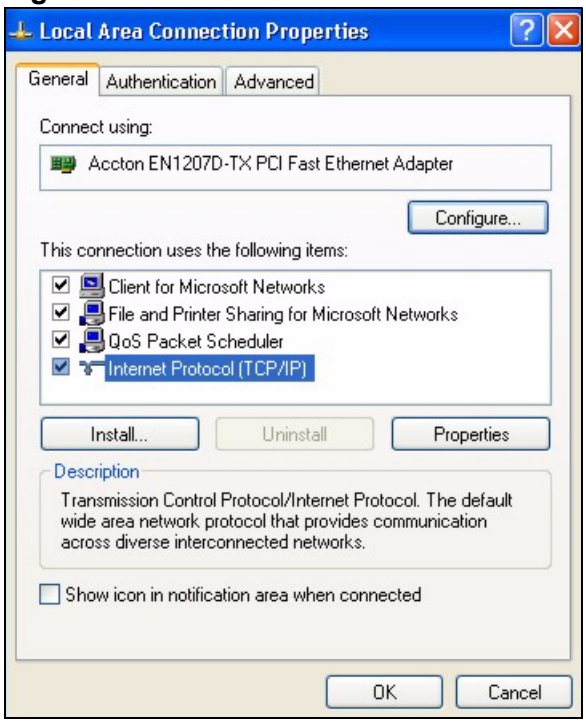
3 Right-click **Local Area Connection** and then click **Properties**.

Figure 78 Windows XP: Control Panel: Network Connections: Properties



4 Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.

Figure 79 Windows XP: Local Area Connection Properties

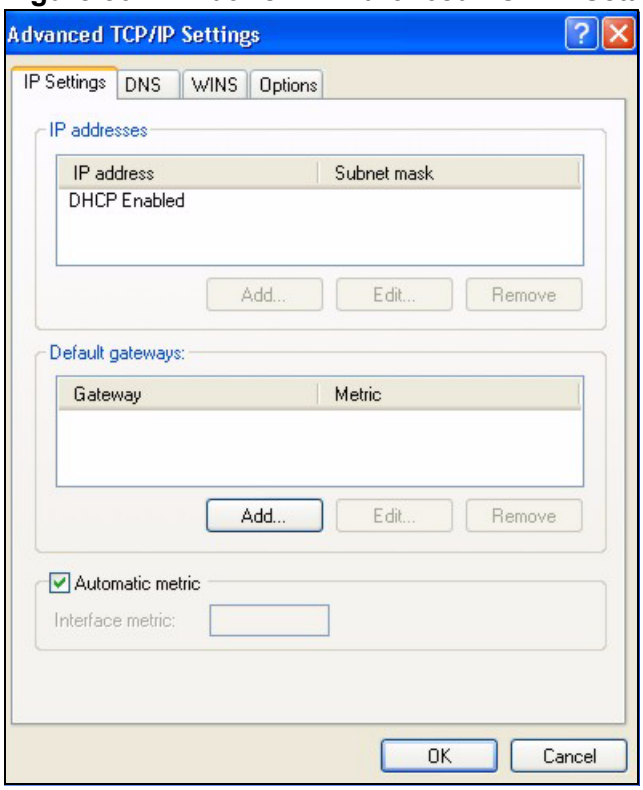

Local Area Connection Properties
General Authentication Advanced
Connect using:
Accton EN1207D-TX PCI Fast Ethernet Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol (TCP/IP)
Install... Uninstall Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

5 The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

- If you have a dynamic IP address click **Obtain an IP address automatically**.

- If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields. Click **Advanced**.

Figure 80 Windows XP: Advanced TCP/IP Settings



6 If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Setting**s tab and click **OK**.

Do one or more of the following if you want to configure additional IP addresses:

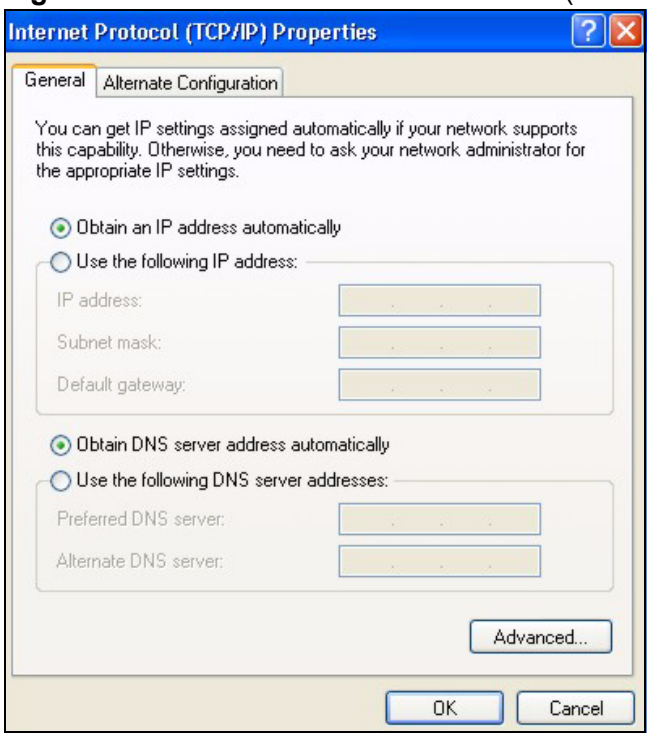
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.
- In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.
- Click **Add**.
- Repeat the previous three steps for each default gateway you want to add.
- Click **OK** when finished.

7 In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

- Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).
- If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

  If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.

Figure 81 Windows XP: Internet Protocol (TCP/IP) Properties


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

10 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

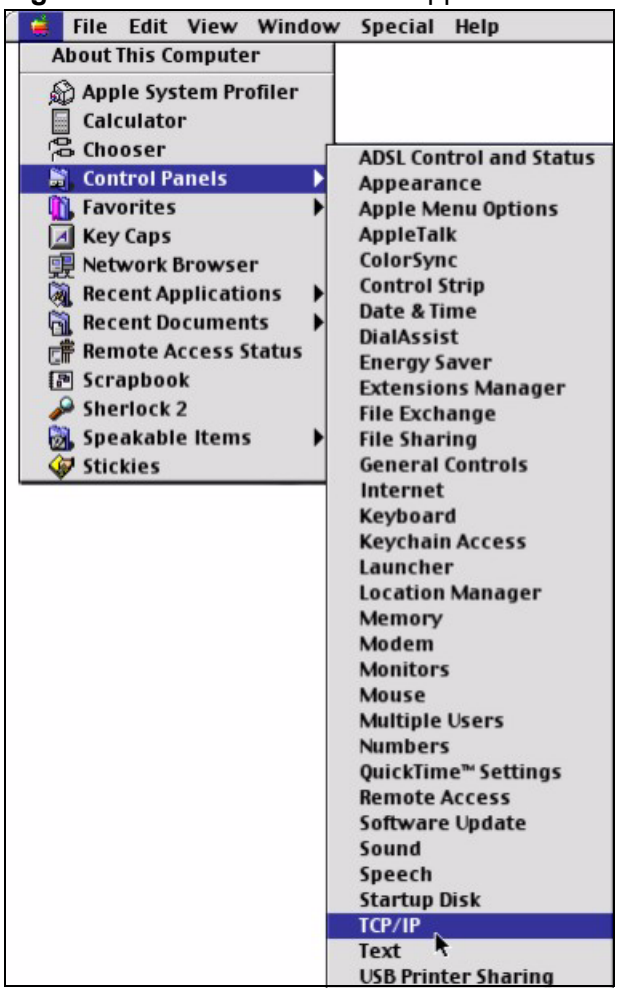
1 Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

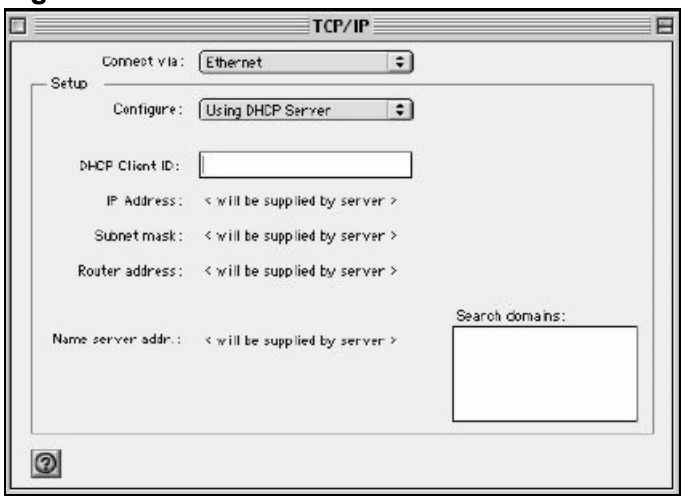
1 Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.

Figure 82 Macintosh OS 8/9: Apple Menu



2 Select **Ethernet built-in** from the **Connect via** list.

Figure 83 Macintosh OS 8/9: TCP/IP



3 For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.

4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Close the **TCP/IP Control Panel**.

6 Click **Save** if prompted, to save changes to your configuration.

7 Turn on your ZyXEL Device and restart your computer (if prompted).

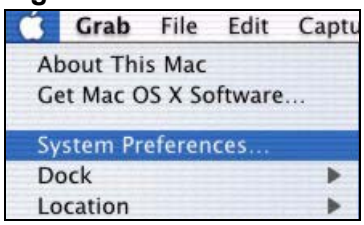
Verifying Settings

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

Macintosh OS X

1 Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.

Figure 84 Macintosh OS X: Apple Menu

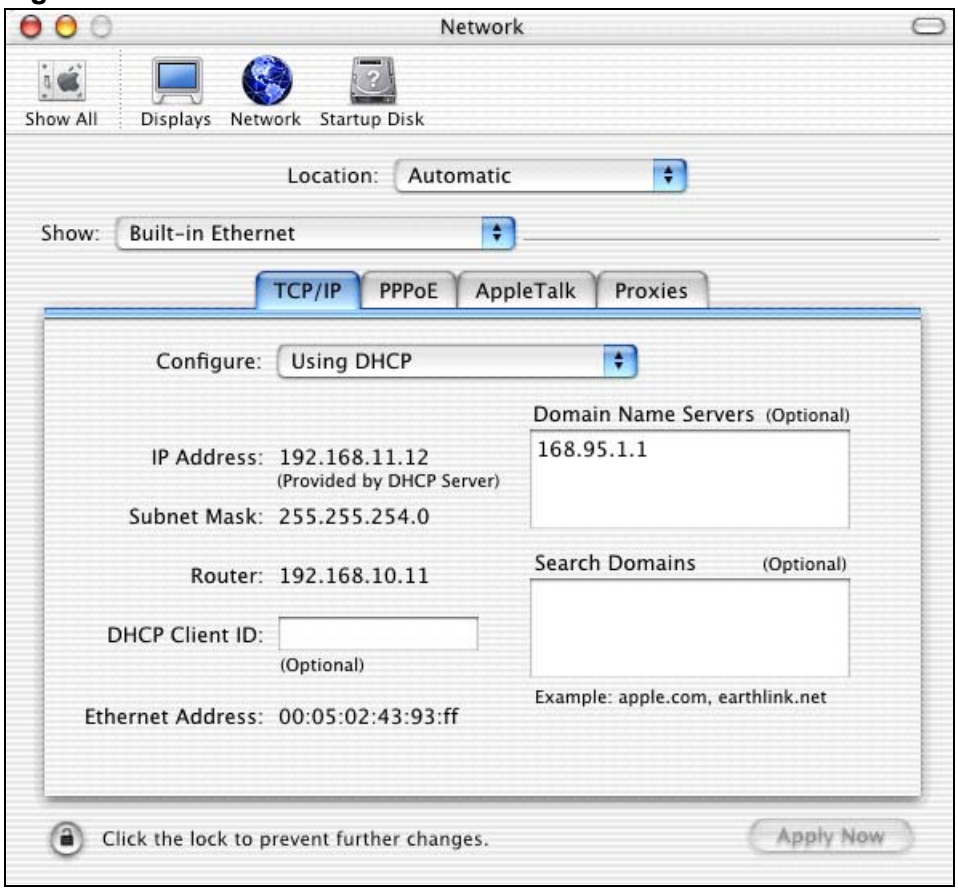


2 Click **Network** in the icon bar.

- Select **Automatic** from the **Location** list.
- Select **Built-in Ethernet** from the **Show** list.
- Click the **TCP/IP** tab.

3 For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

Figure 85 Macintosh OS X: Network



4 For statically assigned settings, do the following:

- From the **Configure** box, select **Manually**.
- Type your IP address in the **IP Address** box.
- Type your subnet mask in the **Subnet mask** box.
- Type the IP address of your ZyXEL Device in the **Router address** box.

5 Click **Apply Now** and close the window.

6 Turn on your ZyXEL Device and restart your computer (if prompted).

Verifying Settings

Check your TCP/IP properties in the **Network** window.

E

Wireless LANs

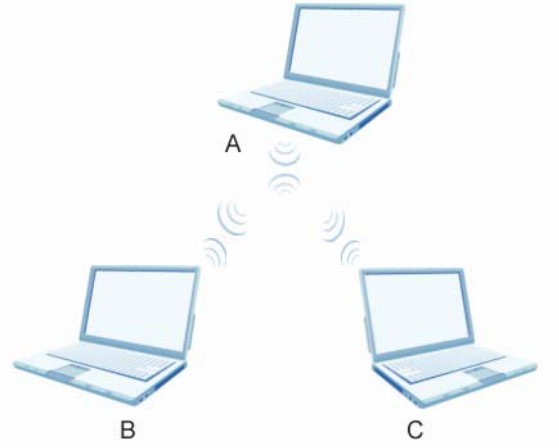
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 86 Peer-to-Peer Communication in an Ad-hoc Network



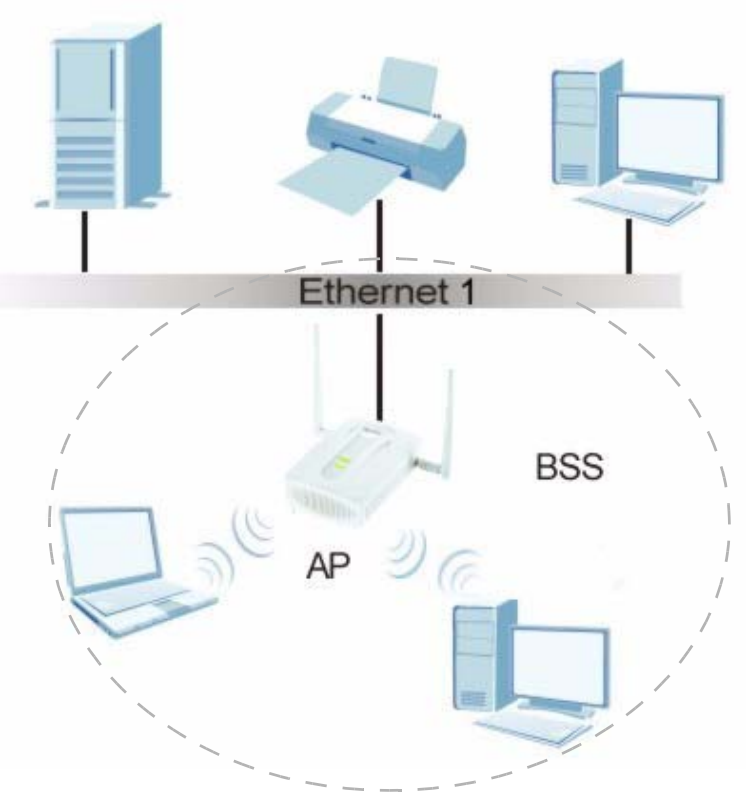
BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate

with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 87 Basic Service Set



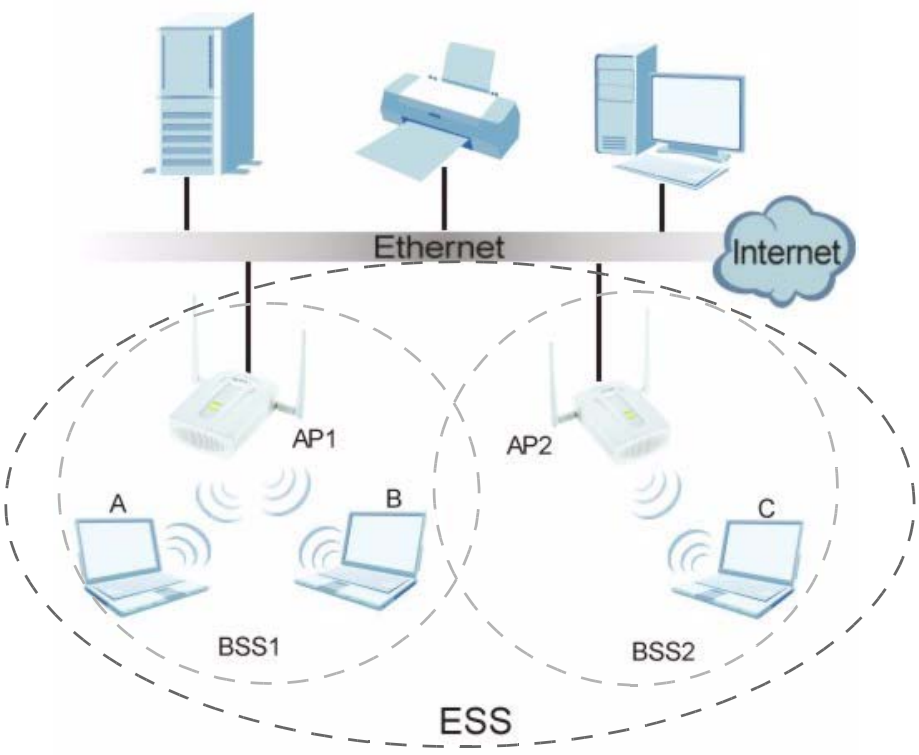
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 88 Infrastructure WLAN



Channel

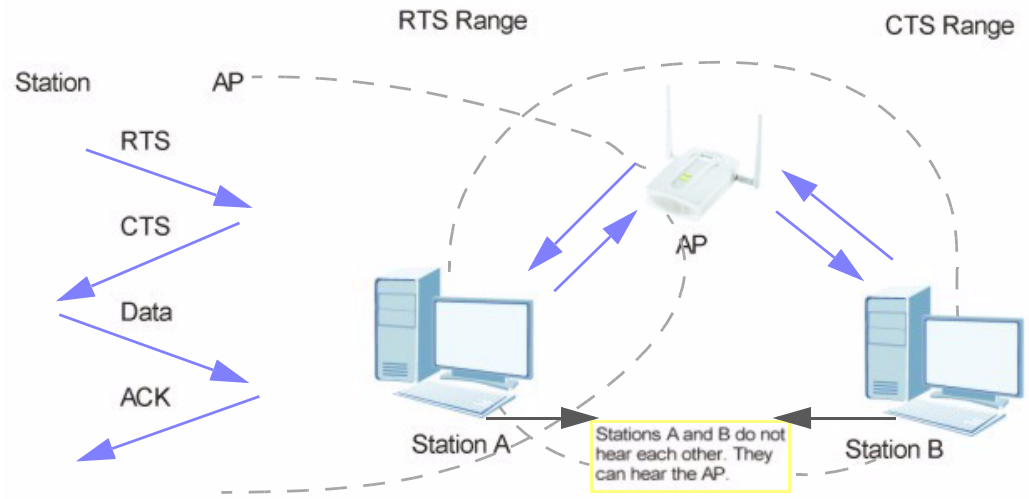
A channel is the radio frequency(ies) used by IEEE 802.11a/b/g wireless devices. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a different channel than an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 89 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 1 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra

network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. **Short** and **Long** refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b/g compliant wireless adapters support long preamble, but not all support short preamble.

Select **Long** preamble if you are unsure what preamble mode the wireless adapters support, and to provide more reliable communications in busy wireless networks.

Select **Dynamic** to have the AP automatically use short preamble when wireless adapters support it, otherwise the AP uses long preamble.

Note: The AP and the wireless adapters MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 53 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the ZyXEL Device are data encryption, wireless client authentication, restricting access by device MAC address and hiding the ZyXEL Device identity.

The following figure shows the relative effectiveness of these wireless security methods available on your ZyXEL Device.

Table 54 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the ZyXEL Device and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.

- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.

- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the Wireless screen. You may still configure and store keys here, but they will not be used while Dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 55 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

Both WPA and WPA2 improve data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA and WPA2 use Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP) to offer stronger encryption than TKIP.

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it’s still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption

keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

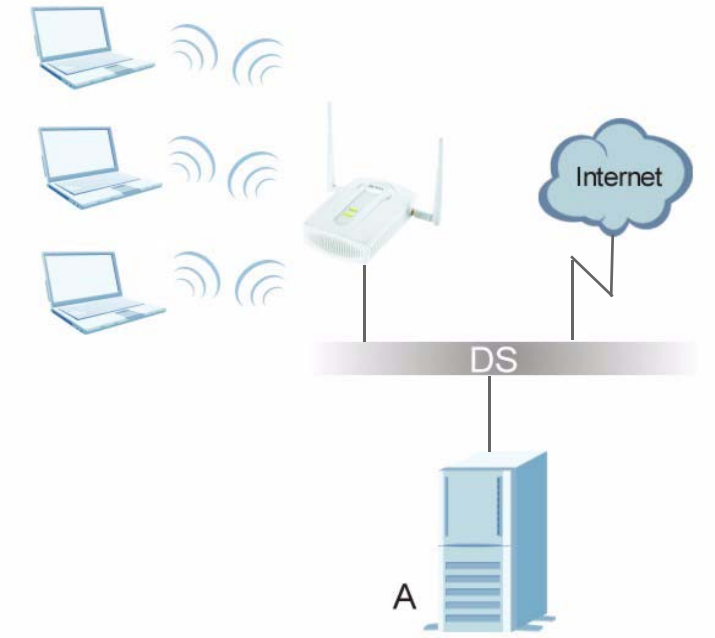
WPA(2) with RADIUS Application Example

You need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.

3 The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the pair-wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 90 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

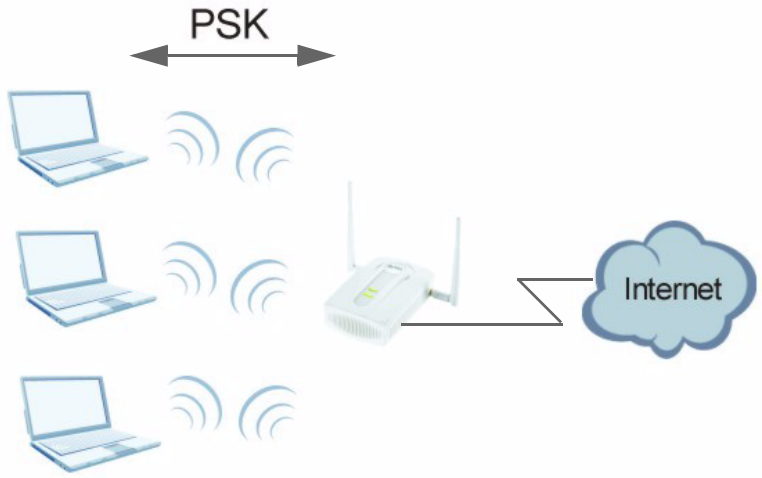
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and (only) allows it to join the network if the password matches.

3 The AP and wireless clients use the pre-shared key to generate a common PMK (Pairwise Master Key).

4 The AP and wireless clients use the TKIP or AES encryption process to encrypt data exchanged between them.

Figure 91 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each Authentication Method/ key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 56 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b) or 5GHz(IEEE 802.11a) is needed to communicate efficiently in a wireless LAN.

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

F

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

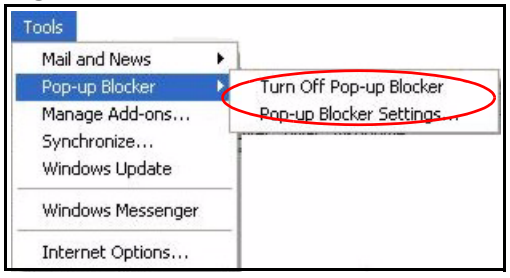
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 92 Pop-up Blocker

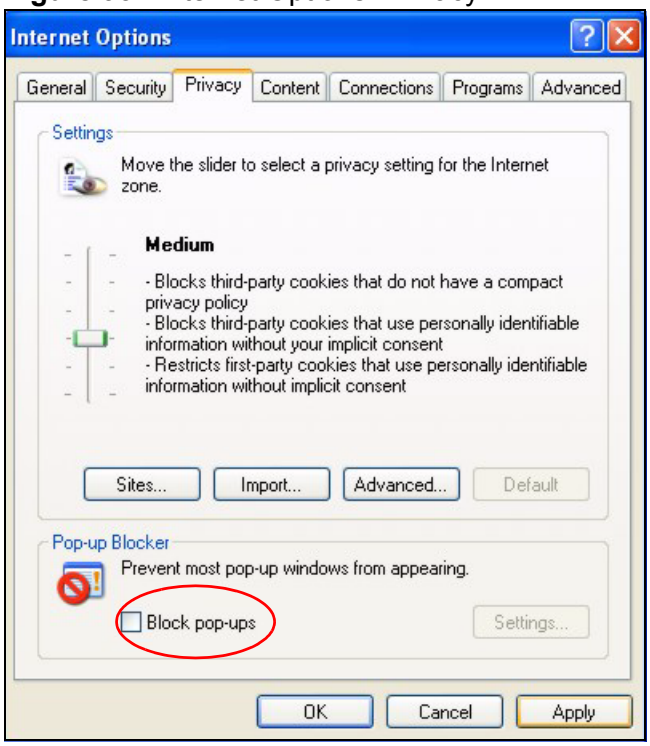


You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 93 Internet Options: Privacy



3 Click **Apply** to save this setting.

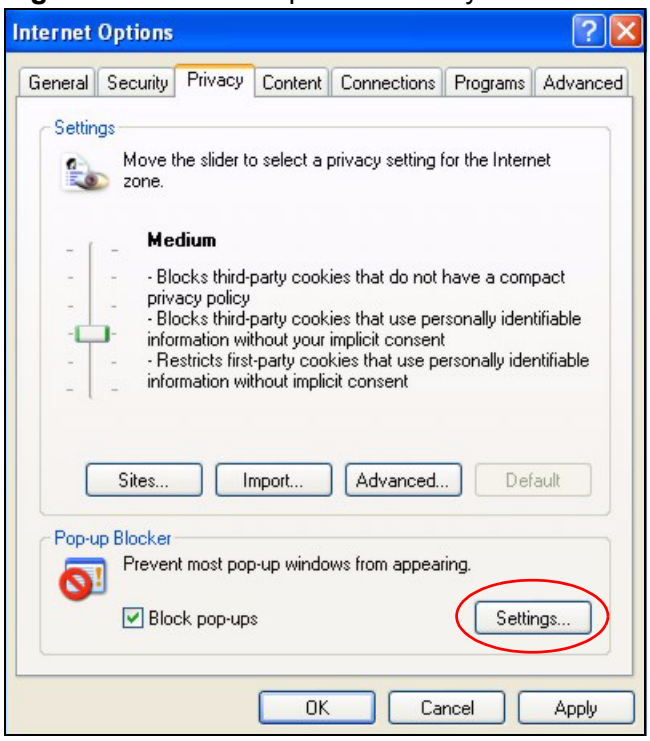
Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 94 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 95 Pop-up Blocker Settings

Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

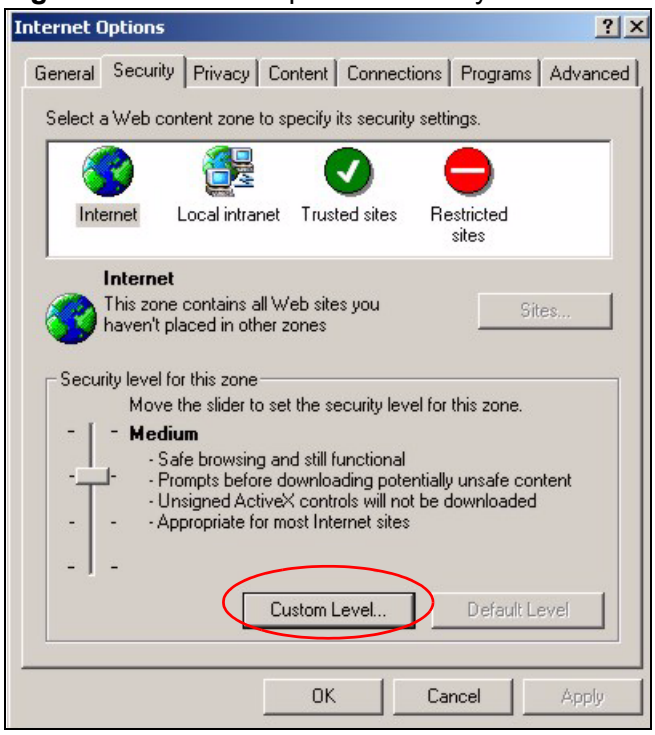
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 96 Internet Options: Security



2 Click the **Custom Level...** button.

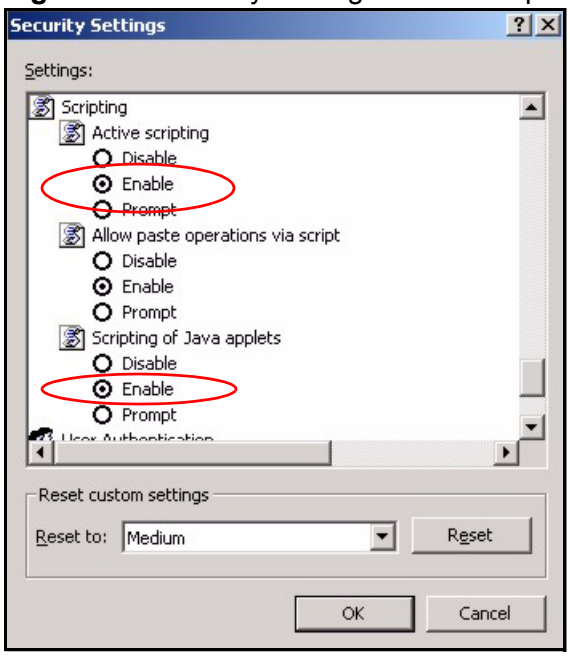
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 97 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

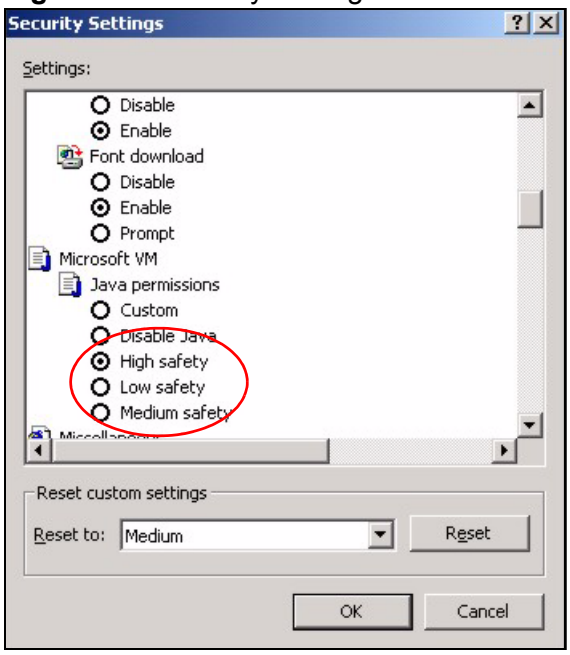
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 98 Security Settings - Java



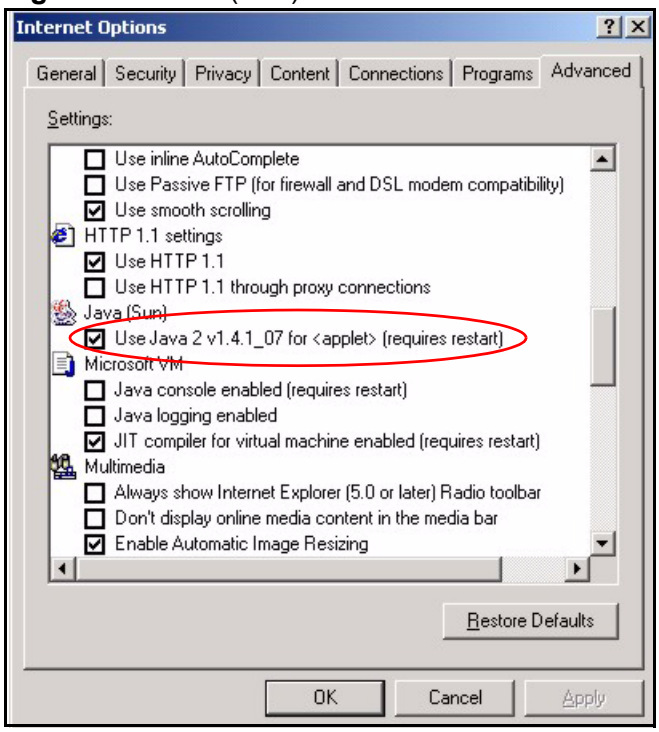
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 99 Java (Sun)



G

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

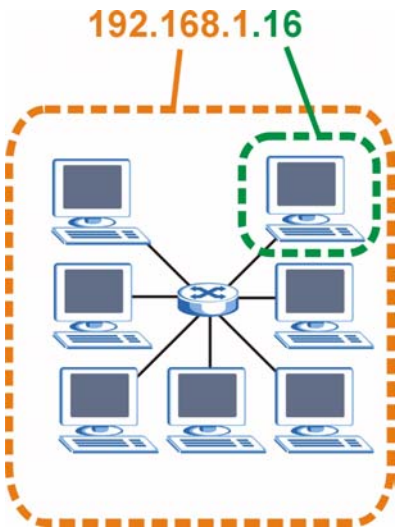
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 100 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term "subnet" is short for "sub-network".

A subnet mask has 32 bits. If a bit in the subnet mask is a "1" then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is "0" then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 57 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000

Table 57 Subnet Masks

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a "1" value). For example, an "8-bit mask" means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 58 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 59 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} - 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} - 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} - 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} - 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 60 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

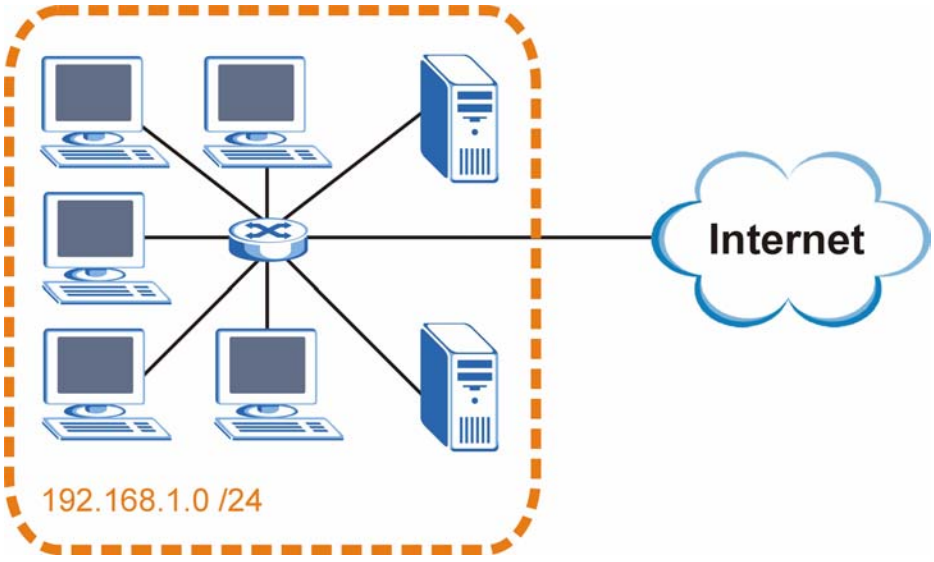
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 101 Subnetting Example: Before Subnetting

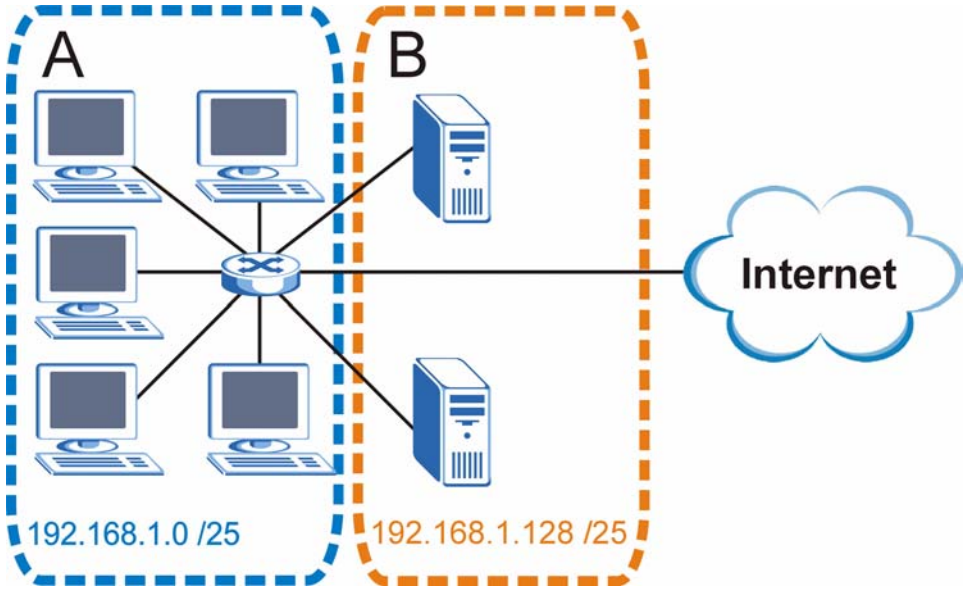


You can "borrow" one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The "borrowed" host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 102 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 61 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 62 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 63 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 64 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000

Table 64 Subnet 4 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 65 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 66 24-bit Network Number Subnet Planning

NO. “BORROWED” HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 67 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the ZyXEL Device.

Once you have decided on the network number, pick an IP address for your ZyXEL Device that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your ZyXEL Device will compute the subnet mask automatically based on the IP

address that you entered. You don't need to change the subnet mask computed by the ZyXEL Device unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space.*

H

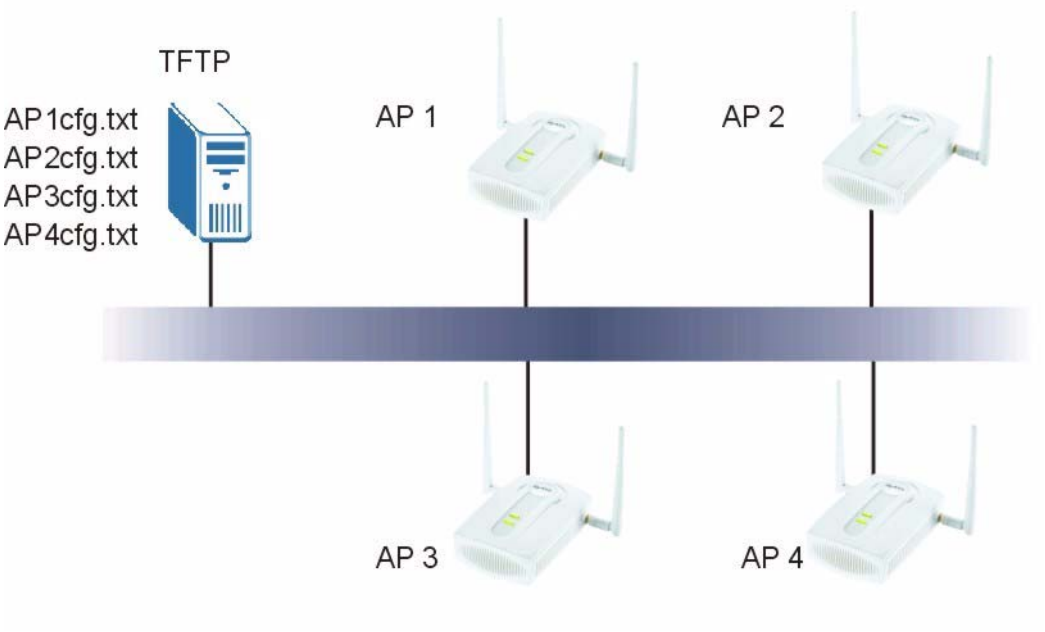
Text File Based Auto Configuration

This chapter describes how administrators can use text configuration files to configure the wireless LAN settings for multiple APs.

Text File Based Auto Configuration Overview

You can use plain text configuration files to configure the wireless LAN settings on multiple APs. The AP can automatically get a configuration file from a TFTP server at startup or after renewing DHCP client information.

Figure 103 Text File Based Auto Configuration



Use one of the following methods to give the AP the IP address of the TFTP server where you store the configuration files and the name of the configuration file that it should download.

You can have a different configuration file for each AP. You can also have multiple APs use the same configuration file.

Note: If adjacent APs use the same configuration file, you should leave out the channel setting since they could interfere with each other's wireless traffic.

Auto Configuration by DHCP

A DHCP response can use options 66 and 67 to assign a TFTP server IP address and a filename. If the AP is configured as a DHCP client, these settings can be used to perform auto configuration.

Table 68 Auto Configuration by DHCP

COMMAND	DESCRIPTION
`wcfg autocfg dhcp [enable | disable]`	Turn configuration of TFTP server IP address and filename through DHCP on or off.

If this feature is enabled and the DHCP response provides a TFTP server IP address and a filename, the AP will try to download the file from the specified TFTP server. The AP then uses the file to configure wireless LAN settings.

Note: Not all DHCP servers allow you to specify options 66 and 67.

Configuration Via SNMP

You can configure and trigger the auto configuration remotely via SNMP.

Use the following procedure to have the AP download the configuration file.

Table 69 Configuration via SNMP

STEPS	MIB VARIABLE	VALUE
Step 1	pwTftpServer	Set the IP address of the TFTP server.
Step 2	pwTftpFileName	Set the file name, for example, g3000hcfg.txt.
Step 3	pwTftpFileType	Set to 3 (text configuration file).
Step 4	pwTftpOpCommand	Set to 2 (download).

Verifying Your Configuration File Upload Via SNMP

You can use SNMP management software to display the configuration file version currently on the device by using the following MIB.

Table 70 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwCfgVersion	1.3.6.1.4.1.890.1.9.1.2	This displays the current configuration file version.

Troubleshooting Via SNMP

If you have any difficulties with the configuration file upload, you can try using the following MIB 10 to 20 seconds after using SNMP to have the AP download the configuration file.

Table 71 Displaying the File Version

ITEM	OBJECT ID	DESCRIPTION
pwTftpOpStatus	1.3.6.1.4.1.890.1.9.1.6	This displays the current operating status of the TFTP client.

Configuration File Format

The text based configuration file must use the following format.

Figure 104 Configuration File Format

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 1 xxx
wcfg security save
wcfg ssid 1 xxx
wcfg ssid save
```

The first line must be `!#ZYXEL PROWLAN`.

The second line must specify the file version. The AP compares the file version with the version of the last configuration file that it downloaded. If the version of the downloaded file is the same or smaller (older), the AP ignores the file. If the version of the downloaded file is larger (newer), the AP uses the file.

Configuration File Rules

You can only use the `wlan` and `wcfg` commands in the configuration file. The AP ignores other ZyNOS commands but continues to check the next command.

The AP ignores any improperly formatted commands and continues to check the next line.

If there are any errors while processing the configuration file, the AP generates a message with the line number and reason for the first error (subsequent errors during the processing of an individual configuration file are not recorded). You can use SNMP management software to display the message by using the following MIB.

Table 72 Displaying the Auto Configuration Status

ITEM	OBJECT ID	DESCRIPTION
pwAutoCfgMessage	1.3.6.1.4.1.890.1.9.1.9	Auto configuration status message string

The commands will be executed line by line just like if you entered them in a console or Telnet CI session. Be careful to ensure the integrity of the whole AP configuration. If there are existing settings in the AP, the newly loaded configuration file will either coexist with the previous settings or replace them.

You can zip each configuration file. You must use the store compression method and a .zip file extension. When zipping a configuration file, you can also add password protection using the same password that you use to log into the AP.

Wcfg Command Configuration File Examples

These example configuration files use the `wcfg` command to configure security and SSID profiles.

Figure 105 WEP Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 11
wcfg security 1 name Test-wep
wcfg security 1 security wep
wcfg security 1 wep keysize 64 ascii
wcfg security 1 wep key1 abcde
wcfg security 1 wep key2 bcdef
wcfg security 1 wep key3 cdefg
wcfg security 1 wep key4 defgh
wcfg security 1 wep keyindex 1
wcfg security save
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 1 l2iolation disable
wcfg ssid 1 macfilter disable
wcfg ssid save
```

Figure 106 802.1X Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 12
wcfg security 2 name Test-8021x
wcfg security 2 mode  8021x-static128
wcfg security 2 wep key1 abcdefghijklm
wcfg security 2 wep key2 bcdefghijklmn
wcfg security 2 wep keyindex 1
wcfg security 2 reauthtime 1800
wcfg security 2 idletime 3600
wcfg security save
wcfg radius 2 name radius-rd
wcfg radius 2 primary 172.23.3.4 1812 1234 enable
wcfg radius 2 backup 172.23.3.5 1812 1234 enable
wcfg radius save
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 2 qos 4
wcfg ssid 2 l2isolation disable
wcfg ssid 2 macfilter disable
wcfg ssid save
```

Figure 107 WPA-PSK Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 13
wcfg security 3 name Test-wpapsk
wcfg security 3 mode wpapsk
wcfg security 3 passphrase qwertyuiop
wcfg security 3 reauthtime 1800
wcfg security 3 idletime 3600
wcfg security 3 groupkeytime 1800
wcfg security save
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 3 qos 4
wcfg ssid 3 l2siolation disable
wcfg ssid 3 macfilter disable
wcfg ssid save
```

Figure 108 WPA Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 14
wcfg security 4 name Test-wpa
wcfg security 4 mode wpa
wcfg security 4 reauthtime 1800
wcfg security 4 idletime 3600
wcfg security 4 groupkeytime 1800
wcfg security save
wcfg radius 4 name radius-rd1
wcfg radius 4 primary 172.0.20.38 1812 20 enable
wcfg radius 4 backup 172.0.20.39 1812 20 enable
wcfg radius save
wcfg ssid 4 name ssid-wpa
wcfg ssid 4 security Test-wpa
wcfg ssid 4 qos 4
wcfg ssid 4 l2isolation disable
wcfg ssid 4 macfilter disable
wcfg ssid save
```

Wlan Command Configuration File Example

This example configuration file uses the `wlan` command to configure the AP to use the security and SSID profiles from the `wcfg` command configuration file examples and general wireless settings. You could actually combine all of this chapter's example configuration files into a single configuration file. Remember that the commands are applied in order. So for example, you would place the commands that create security and SSID profiles before the commands that tell the AP to use those profiles.

Figure 109 Wlan Configuration File Example

```
!#ZYXEL PROWLAN
!#VERSION 15
wcfg ssid 1 name ssid-wep
wcfg ssid 1 security Test-wep
wcfg ssid 2 name ssid-8021x
wcfg ssid 2 security Test-8021x
wcfg ssid 2 radius radius-rd
wcfg ssid 3 name ssid-wpapsk
wcfg ssid 3 security Test-wpapsk
wcfg ssid 4 name ssid-wpa2psk
wcfg ssid 4 security Test-wpa2psk
wcfg ssid save
!line starting with '!' is comment
!change to channel 8
wlan chid 8
!change operating mode -> AP mode,
!then select ssid-wep as running WLAN profile
wlan opmode 0
wlan ssidprofile ssid-wep
!change operating mode -> MBSSID mode,
!then select ssid-wpapsk, ssid-wpa2psk as running WLAN profiles
wlan opmode 3
wlan ssidprofile ssid-wpapsk ssid-wpa2psk
! set output power level to 50%
wlan output power 2
```

How to Access and Use the CLI

This chapter introduces the command line interface (CLI).

Accessing the CLI

Use **Telnet** to access the CLI.

1. Connect your computer to one of the Ethernet ports.
2. Open a Telnet session to the ZyXEL Device's IP address. If this is your first login, use the default values.

Table 73 Default Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Make sure your computer IP address is in the same subnet, unless you are accessing the ZyXEL Device through one or more routers. In the latter case, make sure remote management of the ZyXEL Device is allowed via Telnet.

Logging in

Use the administrator username and password. If this is your first login, use the default values. in some ZyXEL Device models you may not need to enter the user name.

Table 74 Default User Name and Password

SETTING	DEFAULT VALUE
User Name	admin
Password	1234

The ZyXEL Device automatically logs you out of the management interface after five minutes of inactivity. If this happens, simply log back in again. Use the `sys`

`stdio set` command to extend the idle timeout. For example, the ZyXEL Device automatically logs you out of the management interface after 60 minutes of inactivity after you use the `sys stdio set 60` command. Use the `sys stdio show` command to display the current idle timeout setting.

Command Conventions

Command descriptions follow these conventions:

- Commands are in `courier new font`.
- Required input values are in angle brackets <>; for example, `ping <ip-address>` means that you must specify an IP address for this command.
- Optional fields are in square brackets []; for instance in the `show logins [name]` command, the *name* field is optional.

  The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the `contact` field is optional. However, if you use `contact`, then you must provide the *system contact* information.
- The | (bar) symbol means "or".
- *italic* terms represent user-defined input values; for example, in `sys datetime date [year month date]`, *year month date* can be replaced by the actual year month and date that you want to set, for example, 2007 08 15.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "Enter" or "Return" key on your keyboard.
- `<cr>` means press the [ENTER] key.
- An arrow (`-->`) indicates that this line is a continuation of the previous line.

A long list of pre-defined values may be replaced by a command input value 'variable' so as to avoid a very long command in the description table. Refer to the command input values table if you are unsure of what to enter.

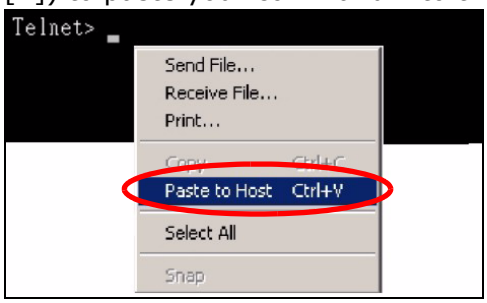
Table 75 Common Command Input Values

LABEL	DESCRIPTION
description	Used when a command has a description field in order to add more detail.
ip-address	An IP address in dotted decimal notation. For example, 192.168.1.3.
mask	The subnet mask in dotted decimal notation, for example, 255.255.255.0.
mask-bits	The number of bits in an address's subnet mask. For example type /24 for a subnet mask of 255.255.255.0.
port	A port number.
hostname	The hostname can be an IP address or domain name.
name	Used for the name of a rule, policy, set, group and so on.
number	Used for a number, for example 10, that you have to enter.

Note: Commands are case sensitive! Enter commands exactly as seen in the command interface. Remember to also include underscores if required.

Copy and Paste Commands

You can copy and paste commands directly from this document into your terminal emulation console window (such as HyperTerminal). Use right-click (not [CTRL]-[V]) to paste your command into the console window as shown next.



Using Shortcuts and Getting Help

This table identifies some shortcuts in the CLI, as well as how to get help.

Table 76 CLI Shortcuts and Help

COMMAND / KEY(S)	DESCRIPTION
▲▼ (up/down arrow keys)	Scrolls through the list of recently-used commands. You can edit any command or press [ENTER] to run it again.
?	Displays the keywords and/or input values that are allowed in place of the ?.
help	Displays the (full) commands that are allowed in place of help.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Use the help command to view the executable commands on the ZyXEL Device. Follow these steps to create a list of supported commands:

1 Log into the CLI.

2 Type `help` and press [ENTER]. A list comes up which shows all the commands available for this device.

```
ras> help
alarm           chsh            config
exit            ip              statistics      switch
sys             voip
ras>
```

Saving Your Configuration

In the ZyXEL Device some commands are saved as you run them and others require you to run a save command. See the related section of this guide to see if a save command is required.

Note: Unsaved configuration changes are lost once you restart the ZyXEL Device

Logging Out

Use the `exit` command to log out of the CLI.

J

Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This product include Hostapd, WPA Supplicant, wireless_tools, vsftpd, busybox, ntpclient, Linux(kernal) and smtpclient under GPL 2.0 License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software

or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty;

keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS. All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

This Product include Redboot software under eCos license

eCos License

This file is part of eCos, the Embedded Configurable Operating System.

Copyright (C) 1998, 1999, 2000, 2001, 2002, 2003 Red Hat, Inc.

Copyright (C) 2002, 2003 John Dallaway

Copyright (C) 2002, 2003 Nick Garnett

Copyright (C) 2002, 2003 Jonathan Larmour

Copyright (C) 2002, 2003 Andrew Lunn

Copyright (C) 2002, 2003 Gary Thomas

Copyright (C) 2002, 2003 Bart Veer

eCos is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

eCos is distributed in the hope that it will be useful, but WITHOUT ANY ARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with eCos; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

As a special exception, if other files instantiate templates or use macros or inline functions from this file, or you compile this file and link it with other works to produce a work based on this file, this file does not by itself cause the resulting work to be covered by the GNU General Public License. However the source code for this file must still be made available in accordance with section (3) of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

This Product include net-snmp and madwifi software under BSD license

BSD

Copyright (c) [dates as appropriate to package]

The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the University nor of the Laboratory may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Note: Some components of the NWA-1100 incorporate source code covered under the BSD License, GPL 2.0 License, eCOs License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: ZyXEL Technical Support.

End-User License Agreement for NWA-1100

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR MONEY WILL BE REFUNDED.

1 1.Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by United States Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL on its Open Source web site (http://www.XXXXXXX.zyxel.com.tw/) (collectively the °×Open-Sourced Components°±) You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components. ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (http://www.XXXXXXX.zyxel.com.tw/), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who

come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL'S AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT°ØS PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8.Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE

IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

8 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

9 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

10 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

K

Legal Information

Copyright

Copyright © 2009 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.

- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1 Reorient or relocate the receiving antenna.

2 Increase the separation between the equipment and the receiver.

3 Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

4 Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz and 5 GHz networks throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or

purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Index

Numbers

802.1x-Only 74
802.1x-Static128 75
802.1x-Static64 75

A

Access Point 20, 39
Accounting Server 91
Ad-hoc 157
Advanced Encryption Standard
  See AES.
AES 167
Alerts 116
Alternative subnet mask notation 184
announcements
  software 203
Antenna 71, 139
  directional 172
  gain 171
  omni-directional 172
  positioning 171
AP (Access Point) 159
AP + Bridge 24
Applications
  Access Point 20
  AP + Bridge 24
  Bridge 21
  Wireless Client 21
Auto Configuration 191
Auto Configuration Status 194

B

Basic Service Set 56
  see BSS
beacon 57
Beacon Interval 59
BPDU 69
Bridge 21
Bridge loops 23
bridged APs, security 21
BSS 56, 157

C

CA 165
Certificate
  authentication 111
  file format 111
Certificate Authority
  See CA.
Certificate Screen 111
certificate-based authentications 166
Certificates
  Fingerprint 114
  MD5 114
  public key 111
  SHA1 114
Certification Authority 113
Certifications 215
  notices 217
  viewing 217
Channel 57, 65, 159
  interference 159
CLI
  accessing the CLI 199
Client authentication 165
command interface 25
Configuration File
  examples 194
  format 193
Configuration File Rules 193
Controlling network access, Ways of 19
Copyright 215
CTS (Clear to Send) 160

D

Date and time start 53
DHCP 50
digital certificate 165
Dimensions 139
Disclaimer 215
Distribution System 56
DNS 47
Domain Name Server (DNS) 47
DS 56
DTIM Interval 60
Dynamic WEP key exchange 166

E

EAP 75
EAP authentication 164
Enable Antenna Diversity 63, 66
Enable Spanning Tree Control (STP) 63
Enable Spanning Tree Protocol(STP) 66
Encryption 75, 77, 80, 84, 166, 167
ESS 56, 158
Ethernet device 94
Ethernet Port 139
Extended Service Set 56
see ESS
Extensible Authentication Protocol 75

F

Factory Defaults 130
restoring 30
FCC interference statement 215
File Version 193
Firmware 123
Firmware, uploading via web configurator 126
Fragmentation 60, 63, 66
Fragmentation threshold 70, 161
FTP 103
restrictions 103

G

Generic Token Card 76
GTC 76

H

handshake 160
help (in the CLI) 201
Hidden node 160
Hide SSID 59
Humidity 139

I

IANA 99, 190
IBSS 157
IEEE 802.11g 162
IEEE 802.1x 57
Import Certificate 112
Independent Basic Service Set
see IBSS
Infrastructure WLAN 158
Initialization vector (IV) 167
interference due to overlap 159
Internet Assigned Numbers Authority 99
See IANA
Intra-BSS Traffic 59
IP Address 48, 97, 139
Arbitrary IP address 48
Gateway IP address 97
IANA 48
ISP 48
Private IP Address Ranges 48
Subnet Mask 48
IP Screen 97
DHCP 98
IPSec VPN capability 140
ISP 99

J

jitter 68

K

key 75, 78

L

latency 68
LEAP 76
LEDs 27, 131
  Blinking 27
  ETHERNET 28
  Flashing 27
  Off 27
  On 27
  SYS 27
  WLAN 27
legacy authentication methods 165
Lightweight Extensible Authentication Protocol 76
Log Commands 121
Log Messages 120
Log Screens 115
Login 199
Logs
  accessing logs 115
  Command List 121
  displaying logs 121
  receiving logs via e-mail 116
Logs Screen
  Mail Server 118
  Mail Subject 118
  Send Log to 118
  Syslog 119
Logs, Uses of 115
loss of messages 160

M

MAC Address Clone 62
MAC Filter
  Allow Association 93
  Deny Association 93
MAC Filter Screen 93
MAC filtering 140
Maintenance 123
  Association List 124
  Backup 128
  Channel Usage 124
  Configuration 127
  F/W Upload 126
  Restart 130
  Restore 128
Management Information Base (MIB) 109
managing the device
  using Telnet. See command interface.
  using the command interface. See command interface.
Media Access Control 94
Message Integrity Check (MIC) 167
message relay 90
Microsoft Challenge Handshake Authentication Protocol Version 2 76
MSCHAPv2 76
MSDU 60

N

NAT 189
Network Time Protocol (NTP) 47
NTP 47

O

open software announcements 203
Operating Mode 56
Output Power Management 60, 62, 65

P

Pairwise Master Key (PMK) 167, 169
Passphrase 75
Password 132, 139
PEAP 76
Personal Information Exchange Syntax Standard 111
PFX PKCS#12 111
PoE 141
Power specifications 139, 141
Preamble 70
Preamble mode 161
Preamble Type 60, 63, 65
Pre-Shared Key 75
Private-Public Certificates 113
Product registration 218
Protected Extensible Authentication Protocol 75
PSK 75, 167

Q

QoS 68
Quality of Service 68

R

Radio Enable 60, 62, 65
Radio Frequency 71
RADIUS 89, 163
  Accounting 90
  Authentication 90
  Authorization 90
  message types 163
  messages 163
  shared secret key 164
RADIUS Screen 89
  Accounting Server 91
  Accounting Server IP Address 91
  Accounting Server Port 91
  Backup 91
  Primary 91
  Server IP Address 91
  Server Port 91
  Share Secret 91
RADIUS server 74
Rates Configuration 60, 63, 66
registration
  product 218
Related documentation 3
Remote Authentication Dial In User Service 89
remote management 25
remote management limitations 102
Reset button 139
Rijndael 167
RJ-45 Port Pin Assignments 141
Roaming 71
root path cost 69
RTS (Request To Send) 160
  threshold 160, 161
RTS/CTS Threshold 60, 63, 65, 70

S

Safety warnings 7
Saving configuration 202
Security Mode, Choosing the 87
Security Modes
  802.1x-Static64 75
  IEEE 802.1x-Only 74
  IEEE 802.1x-Static128 75
  IEEE 802.1x-Static64 75
  None 74
  WEP 74
  WPA 75
  WPA2 75
  WPA2-MIX 75
  WPA2-PSK 75
Service Set IDentifier 57
Share Secret 91
Shortcuts 201
Simple Mail Transfer Protocol 116
Single user account 48
SMTP 116, 118
SNMP 140
  MIBs 109

traps 109
software announcements 203
Spanning Tree Protocol 68
Bridge Protocol Data Units 69
How STP Works 69
Port States 70
Rapid STP 68
Terminology 69
topology 68
Specifications 141
SSID 57
SSL Passthrough 140
Status Screens 33
802.11 Mode 35
Channel ID 35
Ethernet 33
FCS Error Count 35
Firmware Version 34
Interface Status 35
Poll Interval 35
Refresh Interval 34
Retry Count 35
Statistics 35
System Resources 34
system statistics 33
WLAN 33
STP 68
STP (Spanning Tree Protocol) 139
STP-only aware bridges 68
Subnet 181
Subnet Mask 49, 97, 139, 182
subnetting 185
synchronization field 161
Syntax conventions 5
Syslog Logging 116
System Screens 47
General 49
Inactivity Timer 50
System DNS Servers 50
Password 50
Time 51
Daylight Savings 52
NTP client 52
Time and Date Setup 51
Time Server, user-defined 52
Time Zone 52
system timeout 104

T

telnet 104
Telnet (accessing the CLI) 199
Temperature 139
Temporal Key Integrity Protocol 75
Temporal Key Integrity Protocol (TKIP) 167
Text file based auto configuration 140, 191
TFTP restrictions 103
Thumbprint Algorithm 114
Time Servers List 53
timeout 25
TKIP 75
TLS 75
Tracing 140
Trademarks 215
Transport Layer Security 75
Troubleshooting 131
connection is slow or intermittent 134
DHCP 133
factory defaults 133
firmware 134
Internet 134
LAN/ETHERNET port 133
QoS 135
WAN port 133
Web Configurator 132
TTLS 76
Tunneled Transport Layer Security 76
Tutorial 37

U

User Authentication 74

W

WAN IP 99
Warranty 217
note 217
WCFG command 194
WDS Settings 65

Web Configurator 29
Logout 31
password 29
WEP 74
WEP key encrypting 88
Wi-Fi MultiMedia 68
Wi-Fi Protected Access 75, 166
Wired Equivalent Privacy 74
Wireless Association List 140
Wireless Client 21, 41
Wireless client WPA supplicants 168
Wireless LAN, Configuration Overview 37
Wireless Mode 57
Wireless Mode, Choosing the
Access Point 37
AP + Bridge 37
Bridge 37
Wireless Client 37
Wireless Security 26, 162
how to improve 26
Levels 74
Wireless Security Screen 73
802.1x Only 78
Access Point 78
Wireless Client 80
802.1x Static 64-bit, 802.1x Static 128-bit 81
WEP 77
WPA 82
Access Point 83
Wireless Client 84
WPA2 or WPA2-MIX 84
Access Point 85
Wireless Client 86
WPA-PSK, WPA2-PSK, WPA2-PSK-MIX 87
Wireless Settings Screen 55
Access Point Mode 58
Antenna 71
AP + Bridge Mode 67
Bridge Mode 63
BSS 56
Channel 57
ESS 56
Fragmentation Threshold 70
Intra-BSS Traffic 70
Operating Mode 56
Preamble 70
Quality of Service 68
Roaming 71
RTS/CTS Threshold 70
SSID 57
Wi-Fi MultiMedia 68
Wireless Client Mode 61
Wireless Mode 57
WMM QoS 68
WLAN
interference 159
security parameters 170
WMM 60
WMM QoS 60, 68
WPA 75, 166
key caching 168
pre-authentication 168
user authentication 168
vs WPA-PSK 167
wireless client supplicant 168
with RADIUS application example 168
WPA capability to Windows XP 168
WPA2 75, 166
user authentication 168
vs WPA2-PSK 167
wireless client supplicant 168
with RADIUS application example 168
WPA2-MIX 75
WPA2-Pre-Shared Key 166
WPA2-PSK 166, 167
application example 169
WPA2-PSK-MIX 75
WPA-PSK 167
application example 169

Z

ZyXEL Device
Ethernet parameters 98
good habits 26
Introduction 19
managing 25
resetting 30, 130
Security Features 25
What to Log 121